Research Journal of Recent Sciences ISSN 2277-2502
Vol. **3(3),** 60-64, March **(2014)** *Res.J.Recent Sci.*

The Possibilities of Establishing an Innovative Approach with Biometrics Using the Brain Signals and Iris Features

B. Sabarigiri and D. Suganyadevi
Sree Saraswathi Thyagaraja College, Pollachi, INDIA

Available online at: www.isca.in, www.isca.me
Received 23th June 2013, revised 28th August 2013, accepted 25th October 2013

Abstract

In our daily life verify our identities or to decide who somebody is extremely essential. Reliable identification makes life go more smoothly. Automated authentication makes the human recognition achievable. Brain wave signals based biometry is a rising research focus and that it may open novel research directions and applications in the future. The strengths and challenges of electroencephalography (EEG) based biometric system and the mixing of the offered iris modality are described in this paper and the possibilities of deploying powerful multi-modality for real-time biometric systems is proposed.

Keywords: Automated authentication, EEG based biometrics, brain wave signals iris features, multi-modalities.

Introduction

Biometrics is the organized authority of measuring suitable attributes of living individuals or populations to make out lively properties or unique characteristics. Implementing biometrics-based technologies has enhanced in present years and plateful to keep the nation and multi-national enterprises by keeping people and assets, more safe and to limit physical right of entry. Biometrics is having the skill to take a bodily trait as images and signals, compute it, and then use it as evidence of —who you are? A number of biometric traits like fingerprinting, face, voice, DNA, retina, iris and signature are in use within a variety of applications. Every biometric trait has its own merits and demerits. Single modal biometric systems execute person recognition based on single modality. The existing single modal biometrics systems have a variety of troubles such as noisy data, individuality, non-universality, high spoof rate, high fault rate and direct attacks.

A biometric system based upon two or more biometric traits can emphasize the strengths; meanwhile improve the drawbacks, of single modal biometric systems, such systems are called multi modal biometric systems. These are more reliable and provide higher verification rates due to the presence of multiple sensors, and it is expected to be more robust to noise, address the problem of non-universality, improve the matching accuracy and provide reasonable protection against spoof attacks.

Compared to other existing biometrics, iris recognition has gained popularity due to factors such as its superficial high accuracy, quick, robust, fast to compare, non-contact acquisition method, and the availability of low cost sensors due to improvements in technology. However, there are many spoofing techniques evolved to cheat every iris biometric sensor. The spoofing techniques are printed iris images and photographic surfaces, re-played video, fake glass/plastic eye and iris texture printed on contact lenses. Liveness detection is furthermore an important and challenging issue which determines the trustworthiness of biometric system which gives security against spoofing and direct attacks. The proposed method describes the current biometrics in a modern approach and discusses the possibilities of iris along with the brain wave signals and resolves the above said issues also increases the strength of digital biometric community.

Problem Definition

Attacks against biometric systems are grouped into four categories namely, i. Attacks at the user interface (input level) ii. Attacks at the interfaces between modules iii. Attacks on the modules iv. Attacks on the template database.

Iris biometrics finds its applications in crucial high security areas and they are subjected to different types of attacks, the reasons for the attacks are to transform their individual uniqueness, to create violence, to create criminal actions, frauds. A person can use any one of the above described spoofing techniques to change the identity of a genuine person. Therefore, providing security and revocability to the iris biometric at the user interface level is highly problematic. Because, the attack is carried out using artificial biometric samples in the input sensor level or the analog area and outside the digital limits of the system. Hence, digital security mechanisms cannot be used.

Liveness detection procedures are only possible countermeasures against directs attacks in the input sensor level. Liveness detection tests are automated tests, performed to detect whether the obtained biometric sample is from a live human being or not. The sophistication and effectiveness of those countermeasures are directly related to cost and the degree of user inconvenience that can be tolerated in a particular application. The robustness of a liveness technique depends more on how the test is implemented than on what liveness indicator is measured. So, need a plan to launch innovative multi modal modality and its discussions are proposed.

Background Study

The eye, Iris and Optic nerve: The eye is the window to the outside world, which is directly connected to the brain. Your eye is fundamentally a perfect receiver and transmitter. The human retina is transmitting data at roughly 10 million bits per second (1.25mb/s each). The retina is in fact a piece of the brain that has developed into the eye and processes neural signals when it detects light. Ganglion cells transmit information from the retina to the privileged brain centers; other nerve cells within the retina execute the foremost stages of analysis about the world[1,10-12]. Approximately, 1.1 million nerve cells are in the optic nerve, which acts as an intermediate between eye and the brain. Optic nerve is the high speed communication line in human body[2].

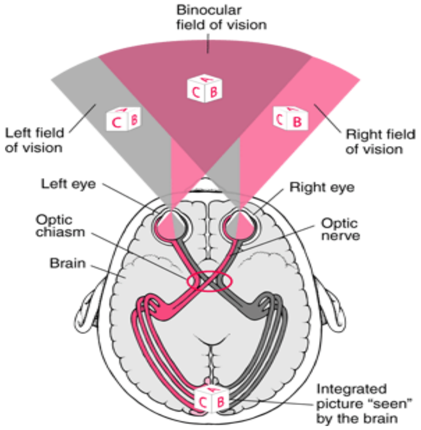

Figure-1
The binocular field of visual travel from eye to brain via optic chiasm

Signals detected by the retina will pass through optic nerve and other nerve fibers (called the visual pathways) to the back of the brain, where vision is sensed and interpreted.

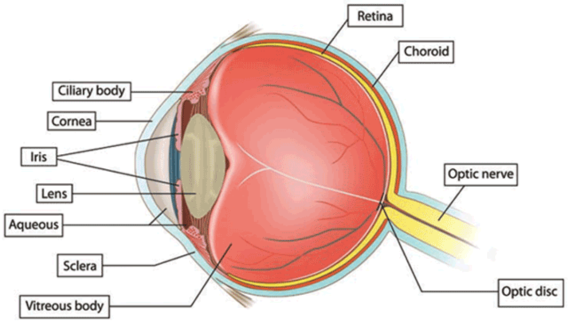

Figure-2
Iris, optic nerve in the eye

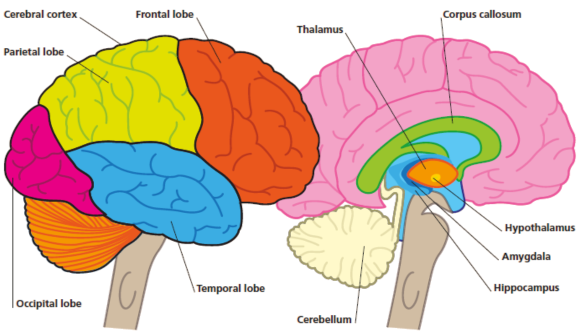

Figure-3
The structure of the brain

The brain: the brain acts as the mid control and data processing unit for the biological medium. Due to the terrific implication of the brain for human life, the brain associated research will have extensive intellectual, societal, economic and health impacts. Cerebrum is divided into the left and right hemispheres and it is responsible for the balance and muscular co-ordination, but its activity cannot be measured by available EEG headsets. They are linked by a central processing unit called the corpus callosum. Each hemisphere is split into four more compartments. They are Occipital lobe, Temporal lobe, Parietal lobe and Frontal lobe. Occipital lobe is back side of the brain in human head and it is dependable for the visual thoughts.

Analysis and Discussion

The following are advantages of multi-modality biometric authentication using iris features and brain wave signals:

Iridology: it claims the pattern, colors, and other characteristics of the iris. Practitioners go with their observations to iris charts (for e.g. figure 4 and 5), which partition the iris into different zones that corresponds to particular parts of the human body[8].

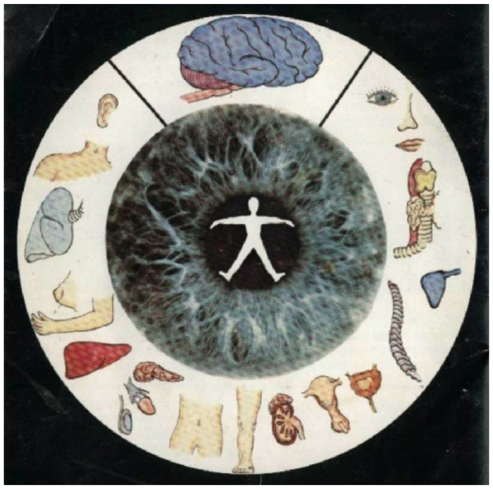

Figure-4
Iris divided into pieces that interconnected with the particular parts of the human body

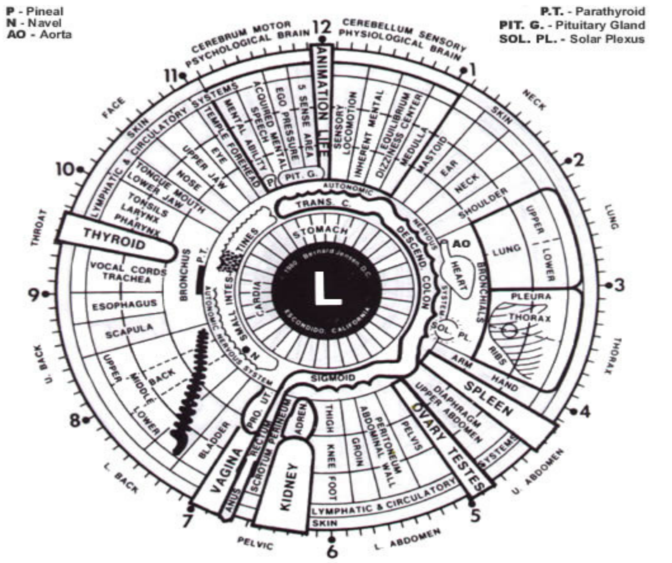

Figure-5
Iris chart

Iridologists measure the body's condition of health. Iridologists believe this information demonstrates a patient's inclination towards certain illnesses, exhibits past medical troubles, or predicts subsequent health problems. The combination of eye, iris, optic nerve, brain motivation will impact in future technologies.

Uniqueness and Stability of Iris: The IRIS patterns are absolute by the eighth month of born, and this pattern wouldn't be changed though out the human being life. The IRIS patterns are unique in nature and the two eyes of an individual contain IRIS pattern which are completely independent from one another are advantages of IRIS. The stability of iris is the key to the identification process[13].

Visual cortex: It's available in the back side of the brain. Occipital lope is accountable for the visual thoughts and which constantly responds to visual stimuli. This part is the most efficient for identification process. This part is accepted as the mainly valuable in conditions of take out unique biometric data.

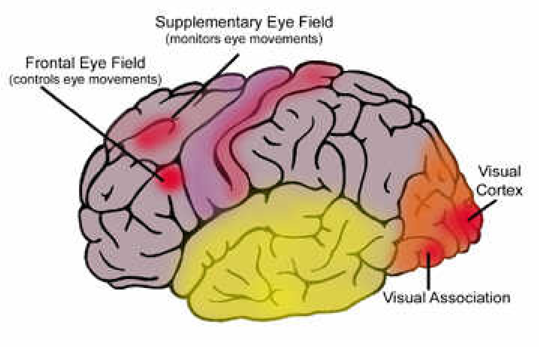

Figure-6
Visual cortex of the brain responds according to the visual stimuli

Low cost sensors: due to improvements in technology gives low cost EEG sensors

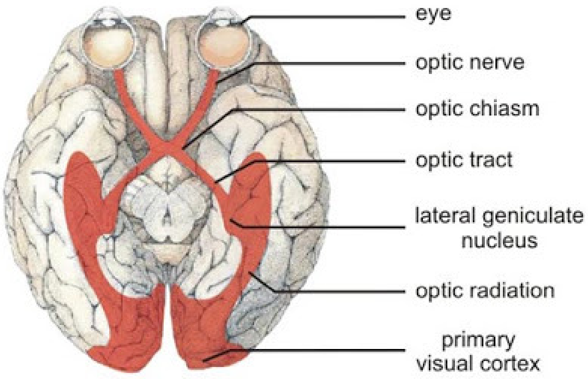

Figure-7
The interconnection between eye and brain

Specific advantages of EEG: i. an effective liveness detection method, ii. EEG which provides the anti-spoofing capability of the existing iris biometric system to meet higher security requirement applications. iii. EEG is not easy to imitate, iv. No one can gain access to the brain waves, because it is safely protected inside the skull. v. Our brain activities are changeable. So this is first changeable biometrics system. vi. EEG signals are particularly strong when a person is exposed to visual stimuli, and the visual cortex area of the brain on the backside of the head is the best place to measure brain-waves, related to the visual sense. The idea of such a system is that instead of using e.g. Normal textual passwords, the system stores a user's personal recording of brain-waves when exposed to self image, and compares this recording to new brain-wave recordings using the self image when the user authenticates prospectively. In this way the system acts as an involuntary challenge-response system. vii. Every individual has a unique and unchanging baseline brain wave patterns[14,15].

While using iris features and brain wave signals for biometric authentication few weakness are identified.

Iris spoofing methods: the iris biometric devices can be spoofed using a variety of methods. the IRIS spoofing[18] methods includes Printed IRIS Images and photographic surfaces, re-played video, fake glass/plastic eye and IRIS texture printed on contact lenses.

Iris Liveness Detection: To reduce the spoof and direct attacks, liveness tests are automated tests performed to establish if the biometric sample presented to a biometric to a recognition came from a live human being or not. The biometric liveness detection fall into three categories (i) the intrinsic properties of a living body (physical/mechanical, electrical, visual, spectral, body fluid) (ii) to analyze involuntary signals generated by a living body (pulse, blood pressure, heat, thermal gradients, corpuscular blood flow signals, skin exudation, transpiration of gases, body odor, perspiration, ECG, EKG, brain wave signals

(EEG), (iii) a challenge-response method, the challenge-responses method can look for either voluntary (behavioral) or involuntary (reflexive) responses. All commercially available iris recognition products contain some level of liveness testing. The sophistication and effectiveness of those countermeasures are directly related to cost and the degree of user inconvenience that can be tolerated in a particular application. The robustness of a liveness technique depends more on how the test is implemented than on what liveness indicator is measured.

Stimuli: to identify the stimuli for a well-organized EEG extraction and capturing the stimulus based EEG brain reaction are more problematical.

User acceptability: if long time to set up the headset, which potentially makes the EEG authentication service impractical and user acceptability will find decreased. Subsequently, identifying the positions affected because of stimuli is more complex.

Recording of EEG: electroencephalography produces a large volume display of brain electrical activity, which creates problems particularly in assessment of long periods recording. Therefore, the detection of the changes in the brain is more complicated. The limitations of these methods, especially when applied to noisy biological data, are now becoming noticeable; their misapplication can simply make fallacious results.

Channel Selection: there are 256 electrode locations are accessible on the scalp. While allowing for all the 256 locations for signal acquisition, the amount of features formed by the system is extremely huge. Preparing the device for all locations and recoding 256 locations is further tedious process. As well as set up the channel locations in the suitable place on the skull without any millimeter changes producing various harms.

Repeated troubles: the difficulty in gathering accurate physiological data lies on whether or not the subject is washed his/her hands, how much gel is applied on his/her electrode, motion artifacts, and precisely where the sensor was placed. The above all facts will make to affect the getting of original data for EEG signal processing, age, day, time, food, psychological status affects the brain wave signals.

Blind people: Obviously, sightless people cannot benefit from an Iris and EEG visual based system authentication.

Artifacts Removal: While extracting the EEG signals the unwanted signals also mixed, they called as “artifacts”. To remove the artifacts is necessary. The artifacts removal techniques will be used for removing the unwanted signals. At that time removing too much of useful information in the EEG signal will give wrong conclusions in the authentication.

Unique features of EEG: Finding the unique features for the purpose of authentication using EEG is highly critical.

Conclusion

Iris is a protected internal organ and has cells that are directly connected to the brain via retina and optic nerve. The integration of iris and EEG recognition biometric systems is to become the leading technology in identity verification. EEG is the spatially weighted summation of all these action potentials measured at the surface of the skull. The technique to extract the human brain information provides a new research paradigm as EEG-based biometry. Furthermore, to overcome the iris liveness detection problems binding the brain waves signals or EEG based biometrics is suggested. To find the solution to all the above said challenges will give an innovative biometric Technology. Iris and EEG are the first of its kind in the international scenario and which provides outstanding identification performance and effective anti-spoofing property.

References

1. The Master Illusionist A Neurological Theory of Psychology By Federico Sanchez **(2010)**
2. www.tedmontgomery.com/the_eye/optcnrve.html **(2013)**
3. http://www.merckmanuals.com/home/eye_disorders/biology_of_the_eyes/structure_and_function_of_the_eyes.html **(2013)**
4. John D., Woodward Jr, Nicholas M. Orlans, Peter T. Higgings, Identity assurance in the information age biometrics, McGraw Hill **(2002)**
5. Kara Rogers, The human body: The eye the physiology of human perception, Britannica Educational Publishing and association with Rosen educational services **(2010)**
6. Light and eyes and vision, Physics of the human body biological and medical physics, biomedical engineering, 629-711, Springer, **(2007)**
7. Juris Klonovs, Christoffer Kjeldgaard Petersen, Henning Olesen, and Allan Hammershoj, ID Proof on the Go-Development of a Mobile EEG based Biometric Authentication System, *IEEE Vehicular Technology Magazine*, March **(2012)**
8. http://en.wikipedia.org/wiki/Iridology **(2013)**
9. http://micro.magnet.fsu.edu/primer/lightandcolor/humanvisionintro.html **(2013)**
10. http://www.uniteforsight.org/course/eyeanatomy.php **(2013)**
11. http://virtualgardneranatphys.wikispaces.com/Sight **(2013)**
12. http://www.glaucoma.org/glaucoma/anatomy-of-the-eye.php **(2013)**
13. Sabarigiri B. and Karthikeyan T., Countermeasures against IRIS spoofing and liveness detection using electroencephalogram (EEG), IEEE International

Conference on Computing Communication and Applications, **(2012)**

14. Juris Kļonovs, Christoffer Kjeldgaard Petersen, Development of a Mobile EEG-Based Feature Extraction and Classification System for Biometric Authentication, **(2012)**

15. Sabarigiri B., Suganyadevi D., Countermeasures against iris direct attacks using fake images and liveness detection based on electroencephalogram (EEG), ICDMSCT, **(2014)**