Encyclopedia of Computer Graphics and Games

Brain Signals as a New Biometric Authentication Method Using Brain-Computer Interface

Fares Yousefi[1] and Hoshang Kolivand[1]

(1)Department of Computer Science, Faculty of Engineering and Technology, Liverpool John Moores University (LJMU), Liverpool, UK

Fares Yousefi (Corresponding author)
Email: f.yousefi@2017.ljmu.ac.uk

Hoshang Kolivand
Email: H.Kolivand@ljmu.ac.uk

Without Abstract

Synonyms

Biometric authentication; Brain-computer interface; EEG signal

Definitions

Human biometric techniques are presented as another type of security authentication to cover the problems of password authentication. Brainwave is another human biometric, which recently is one of the popular subjects for scientists and researchers. Brain-computer interface (BCI) is a method of communication based on neural activity's communication created by the brain.

Introduction

In the past, people used to have a suitcase to keep their important documents like keys, money, bank account booklets, letters, photos, etc. which they could lock the suitcase to keep them secure. Today, people can keep all of that information in their personal computers, mobile devices, social networks, and the cloud storages, which in this case, information security and data protection play a crucial role in them. Security and accurate authentication methods have become a top priority within information security, which is necessary as it allows companies and people to keep their systems and devices protected by authorizing only authenticated users to use important resources (*Margaret*). There are several methods of authentication (*Darril*) such as something you know (password or PIN), something you have (smart card, common access card (CAC) (DeBow and Syed *2016*), personal identity verification (PIV) (Kittler et al. *2002*), or RSA token (*Vangie*)), and something you are (using biometrics). Password or PIN authentication and different kinds of smart cards and

tokens are easy to implement but because of this ease can be very easily stolen or lost. Biometrics is a new technological alternative to solve this problem (Jain et al. *1999*). These typical biometric authentication technologies have some disadvantages (*Erden*). Therefore, a new biometric method needs to be produced to reduce the number of disadvantages that are within current systems. Brain signal is a human's characteristic, which does not have the problem of visibility to copy it, and it does not have the disadvantages of other biometric systems if the authors could employ it as a biometric authentication. Human brain signals are one of the characteristics that, nowadays, scientist and researchers are working on using brain-computer interface (BCI). BCIs are systems that provide communications between human beings and machines.

In the past, people always liked to read each other's mind or it was a wish for them to control their environments or replace objects with their brainpower. Today technology made those dreams happen. For instance, transfusing signals straight to someone else's brain to allow them to experience new sensory inputs like sight, hearing or feel. One of the potential outcomes of the future could be the manipulation of computers and associated devices with the simple transferring of a thought. Considering this potential BCI could be a very significant breakthrough within technology. BCIs are becoming increasingly popular in medical and nonmedical areas as a way of communication to be conducted between humans and machines. Nowadays brain signal authentication using BCI devices is one of the popular subjects for researchers.

This article is a survey about biometric authentication techniques and using brain signals via BCI technologies as a new biometric authentication technique of a human body, which could be the most secure technology in the future.

Overview on EEG Signals

A review about biometric authentication in a couple of research papers and a literature review about BCI and brain signal authentication from the previous experiences of the other researchers, which are categorized to different subjects and goals, are as follows:

Biometrics

The word biometrics is a combination of two Greek words, "bios" (life) and "metrikos" (measure). This technology is mostly used for access control and identification or for identifying people who are under investigation (Faundez-Zanuy *2006*). There are two different concepts in biometrics, which the authors should concentrate on, behavioral/physical biometrics and authentication/identification. Behavioral biometrics concentrates on analyzing the nonphysiological or non-biological structures of any human. It studies the unique psychological characteristics of humans like signature, voice, gait, and keystrokes. Physical biometrics is doing the opposite, which is focusing on analyzing the physiological and biological structures of the human (Agrafioti et al. *2009*). As you can see in Fig. 1, there are a couple of different behavioral and physiological human biometric types.
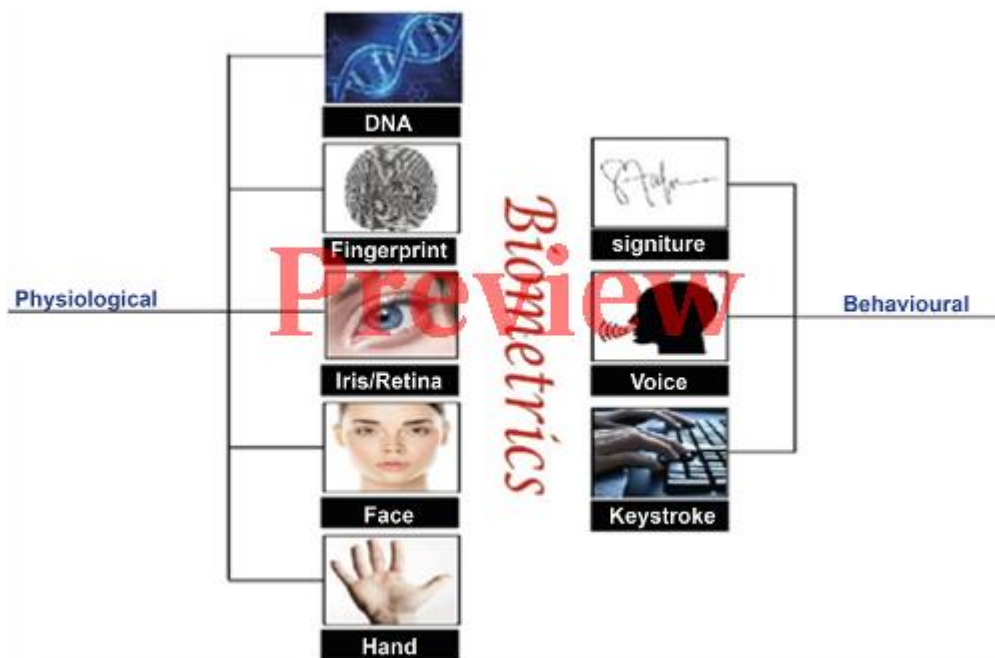
Fig. 1
Physiological and behavioral biometric types

Biometric Authentication Types, Advantages, and Disadvantages

A biometric technique can work in two modes, authentication and identification, which are the heart of the biometric science (Prasanna et al. *2012*). Biometric authentication is one of the most popular ways to provide personal identification because these characteristics of a human are specific and unique. Most of these specific features are so hard to duplicate and accurately produce (Kodituwakku *2015*). In terms of information security, physiological biometric traits appear more practical. The most popular physiological biometric techniques are as follows:

Face Recognition

In comparison with the different biometric identification techniques, "face recognition is one of the most flexible, working even when the subject is unaware of being scanned" (Jafri and Arabnia *2009*). It works by methodically analyzing particular characteristics that are common to human's face such as the size of the nose, the space between the eyes, position of cheekbones, jawline, and so forth (*Margaret*, Facial recognition). Table 1 shows some specific advantages and disadvantages of this biometric technique (Masupha et al. *2015*).**Table 1**
Face recognition biometric advantages and disadvantages

Face recognition	
Advantages	Disadvantages

Prevent card counters, etc. from entering casinos	Isn't accurate at all times
	Hindered by masks, glasses, long hair, etc.
	Pictures must be taken when the users have a neutral face
Identify criminals, terrorists, etc.	
Find missing people	"Considered an invasion of privacy to be watched"
Prevents elector frauds	
Targets shoppers	Easy to abuse

Fingerprint Identification

Fingerprints are the most famous biometric which remain constant throughout life. It is more than 100 years in worldwide fingerprint comparison that no two same fingerprints were found. "Fingerprint identification involves comparing the pattern of ridges and furrows on the fingertips, as well as the minutiae points (ridge characteristics that occur when a ridge splits into two, or ends) of a specimen print with a database of prints on file" (Kute and Kumar *2014*). Table 2 shows some specific advantages and disadvantages of this biometric technique (*Tarun*).**Table 2** Fingerprint biometric advantages and disadvantages

Fingerprint identification	
Advantages	**Disadvantages**
It is one of the most developed biometrics	It needs more computer memory to store scanned data
Very high accuracy	
Easy to use	
Is the most economical biometric PC user authentication technique	Using the fingerprint scanner does not take into consideration when a person physically changes
It is standardized	

Small storage space required for the biometric template, reducing the size of the database memory required	It can make mistakes with the dryness or dirtiness of the finger's skin, as well as with the age (is not appropriate with children, because the size of their fingerprint changes quickly)

Retina Scan

In the backside of the eyeball, there is a layer of cells, which is the retina. This part of the eye converts light into nerve signals. To replicate a retina, there is no known way discovered. The pattern of the blood vessels at the back of the eye is unique. It stays the same for the whole lifetime (Choraś *2012*). Table 3 shows some specific advantages and disadvantages of this biometric technique (*Jatin*).**Table 3**
Retina biometric advantages and disadvantages

Retina scan	
Advantages	**Disadvantages**
Like fingerprints, retina traits remain stable throughout life	Retina scan enrolments take longer than both iris scan and fingerprinting
Its resistance to false matching or false positives, regarding to pupil movements	Users claim discomfort with eye-related technology in general and the fact that retina scan technology has limited uses
The eye from a dead person would deteriorate too fast to be useful, so no extra precautions have to be taken with retinal scans to be sure the user is a living human being	Users commonly fear that the device itself or the light inside the device can harm their eyes in some way
	Users claim discomfort with the fact that they must position their eye very close to the device
The retina is located deep within one's eyes and is highly unlikely to be altered by any environmental or temporal condition	Many also feel that these retina scans can be linked to eye disease

Iris Scan

Iris is another part of the eyes, which has complex patterns that are stable, unique, and, in compare to the retina, can be observable from a long distance. The pattern-recognition method in Iris Scan process is using video images from a person's iris. In iris identification, the probability of error is the lowest of all biometrics. (Shekar and Bhat *2015*). Table 4 shows some specific advantages and disadvantages of this biometric technique (*Biometrictoday*).**Table 4**
Iris biometric advantages and disadvantages

Iris scan	
Advantages	**Disadvantages**
Scalability: This technology is highly scalable and can be used in both large- and small-scale programs	**Distance:** Iris is small and cannot be located from a few meters distance
Accuracy: Iris recognition is one of the best biometric modalities in terms of accuracy	**Expensive:** Iris scanners are relatively higher in cost compared to other biometric modalities
Stable: Iris patterns remain stable throughout an individual's life. It is protected by the body's own mechanism	**Infrared light:** The constant use of this system may cause harm to the iris because it is constantly being scanned with infrared light
Noninvasive: Iris recognition can be done with simple video technology. No use of laser technology is necessary to scan the iris making it a noninvasive technology altogether	**Movement:** A person has to be steady in front of the device to be enrolled by iris scanners. It means this device cannot be used like face recognition devices to scan anybody, regardless of their movements
Easy to use: Iris recognition system is plug and play compared to other modalities of biometric recognition. A person needs to stand still in front of the camera, and the job is done instantly. It is a comfortable process for everyone	**Obscure:** Eyelashes, lenses, and reflections, which create a problem, more often than not, obscure it
Fast: With iris recognition system, a person can complete the process within just a few seconds	**Reflection:** In some cases, it is hard to perform an iris scan due to the presence of reflections. It could happen in case of eyelashes, lenses, and anything in general that would cause a reflection
Traceable: The encoding and decision making of iris pattern is traceable. It takes only 30	**Memory space:** A lot of memory is required for the data to be stored and later accessed

milliseconds for the image analysis and the subsequent encoding	**Transformation:** Iris may deform nonelastically as the pupil may change its size due to medical or other conditions

Current Biometric Technique Advantages and Disadvantages

Biometrics have too many different techniques and methods. After investigating some of the physiological biometric methods and the specific advantages and disadvantages of them, the authors are going to peruse the current biometric technique's advantages and disadvantages. Table 5 shows advantages and disadvantages of recent biometric methods (Le and Jain *2009*).**Table 5** Biometric methods' advantages and disadvantages
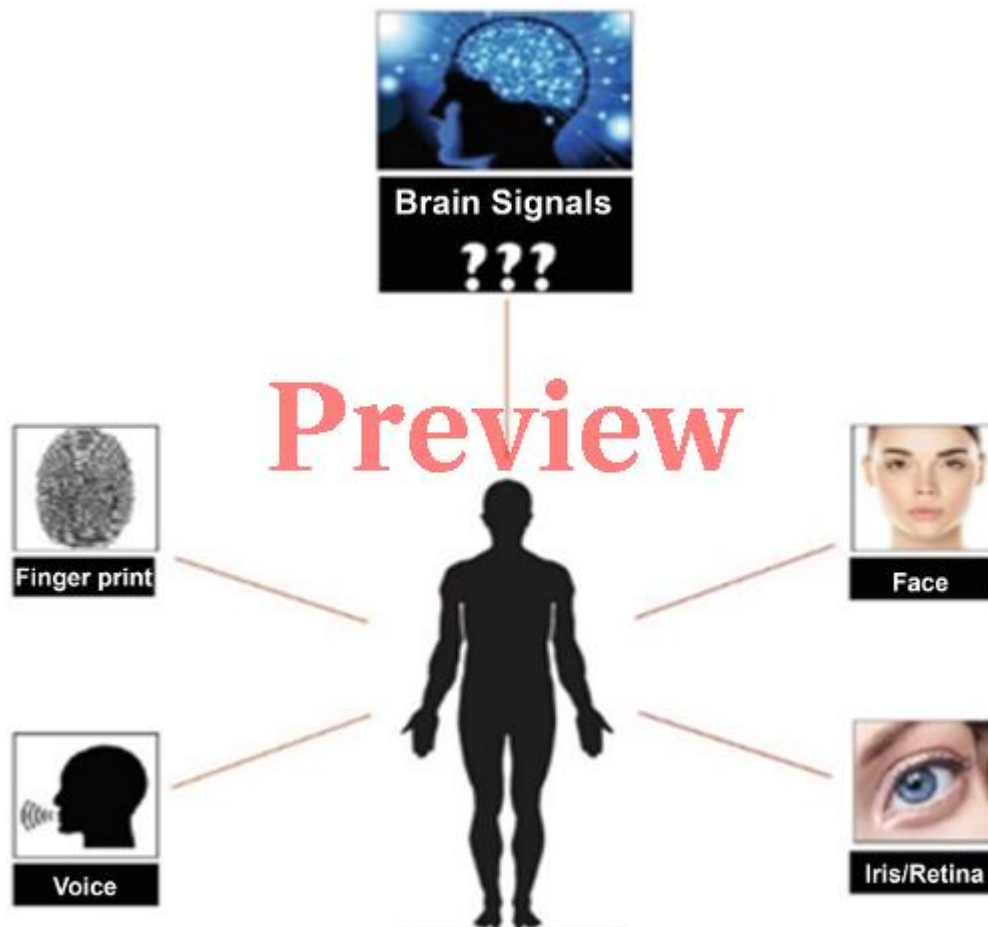
Biometric advantages and disadvantages	
Advantages	**Disadvantages**
Convenient: The credentials are with human forever, so it does not require you to memorize or note down anything	**Physical traits are not changeable:** Users can reset a password, but they never can change their fingerprints or retina; these are fixed
Security: Biometric technology brings different types of solutions, which are nearly impossible to hack unlike passwords	**Unhygienic:** In contact-based biometric techniques, a biometric device is used a lot of times by enormous amount of people. Everyone is actually sharing his or her germs with each other via the device
Scalability: Unlike other solutions, biometrics are highly scalable solutions for all types of projects. It is possible for any kinds of projects because of the scalability of its solutions	**Error rate:** Usually, biometric devices make two types of errors, false acceptance rate (FAR) and false rejection rate (FRR) (Wayman et al. *2005*). When the device accepts an unauthorized person, it is known as FAR, and when it rejects an authorized person, it is known as FRR
Accuracy: Biometric works with individual's physical traits such as fingerprints, face, and retina among others that will always serve you accurately anywhere, anytime	**Delay:** Some biometric devices take more than the accepted time and a long queue of workers form waiting to be enrolled in large companies
Flexibility: People have their own security credentials with you, so you do not need to bother memorizing awkward alphabets, numbers, and symbols required for creating a complex password	**Environment and usage matters:** Environment and usage can affect the overall measurements taken

Save money: With a little money, any company can track their employees and reduce the extra costs they are paying for years	**Physical disability:** Some people are not fortunate enough to be able to participate in the enrolment process. They might have lost or damaged body parts such as fingers or eyes
Save time: Biometric solutions are highly time conserving	
Trustable: Reports claim that the young generations trust biometric solutions more than other solutions	

Brainwaves as a New Biometric Authentication

The potential for using brainwaves as human biometric identification has risen to the surface once again, an idea presented as a way to distinguish humans with thoughts. Before becoming a method of security, it could be the measuring standard for biometric identification in the near future, but it needs more time and work on it. Brain signal can be one of the most practical biometric authentication methods (Fig. 2). It is obviously a possible technique of identification, and in terms of security, it could have a big role to play in the feature.

Neural Oscillations (Brainwaves)

Neural oscillations or brainwaves are an essential mechanism to enable the synchronization of neural activity inside and around brain areas and help the accurate temporal organization of neural processes underlying memory, cognition, behavior, and perception (Neustadter et al. *2016*). "The interaction between neurons can give rise to oscillations at a different frequency than the firing frequency of individual neurons" (Roux and Uhlhaas *2014*).
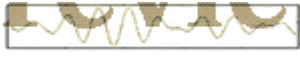
Electroencephalography (EEG)

Hans Berger was a German psychiatrist who observed the first human neural oscillations as early as 1924. He invented electroencephalography (EEG) for the recording of "brainwaves" by measuring electrical activity in the patient's brains in the hospital which had a skull damage (Millet *2002*). EEG is one of the techniques for brain imaging. Table *6* shows the different brain imaging techniques (*Imotion EEG packet guide*).**Table 6**
The methodology of brain imaging techniques and the ways that they work

Brain imaging techniques		
Methodology	**What is imaged?**	**How?**
Electroencephalography (EEG)	Changes in electrical brain current	Electrodes placed on scalp measure electrical brainwaves
Positron emission tomography (PET)	Emissions from radioactive chemicals in the blood	Radioactive isotopes injected into the blood are detected like X-ray
Computed (axial) tomography scan (CT or CAT)	X-ray images of the brain	Multiple images (tomograms) are taken by rotating X-ray tubes. Doesn't image function
Functional magnetic resonance imaging (fMRI)	Blood flow; oxyhemoglobin-to-deoxyhemoglobin ratio	Relies on the magnetic properties of

		blood. Shows brain function spatially and temporally
Magnetoencephalography (MEG)	Changes in electrical brain current	Similar to EEG but magnetic brainwaves are measured instead of electrical brainwaves

Electroencephalography (encephalon = brain) or EEG is an electrophysiological observing technique to capture electrical activity generated by the brain from electrodes placed on the scalp surface (Niedermeyer and da Silva, 2005). "EEG refers to the recording of the brain's spontaneous electrical activity over a period, as recorded from multiple electrodes placed on the scalp" (Niedermeyer and da Silva 2005). Many of the brain's emotion recognition techniques have been implemented and proposed for the last few years which most of them involved the extraction of EEG signals (Abuhashish et al. 2015). In comparison to other imaging methods, EEG has some benefits. It is an excellent tool for studying the processes of neurocognitive underlying person behavior because of some reasons such as the following: (1) EEG has very high time resolution and captures cognitive processes in the time frame in which cognition occurs. (2) EEG directly measures neural activity. (3) EEG is inexpensive, lightweight, and portable. (4) EEG monitors cognitive-affective processing in the absence of behavioral responses (Catarino et al. 2011). In terms of frequency, there are five types of brainwave (gamma, beta, alpha, theta, delta), and "each frequency is measured in cycles per second (Hz) and has its own set of characteristics representing a specific level of brain activity and a unique state of consciousness" (Korde and Paikrao 2018). This is represented in Table 7. According to the types of brainwaves, four different kinds of mental activities such as movement, emotions, talking, and motor imagery have been measured by investigators (Abuhashish et al. 2014).**Table 7** Types of brainwaves and their frequency rates and mental state situation

Wave	Frequency	Mental state
Gamma	Above 40 Hz **If you need to edit the image, please use the original: 326336_0_En_370-1_Figa_HTML.gif**	Thinking, integrated thought
Beta	13–40 Hz **If you need to edit the image, please use the original: 326336_0_En_370-1_Figb_HTML.gif**	Alertness, focused, integrated, thinking, agitation, aware of self and surroundings
Alpha	8–12 Hz	Relaxed, non-agitated, conscious state of mind

	If you need to edit the image, please use the original: 326336_0_En_370-1_Figc_HTML.gif	
Theta	4–7 Hz **If you need to edit the image, please use the original: 326336_0_En_370-1_Figd_HTML.gif**	Intuitive, creative, recall, fantasy, dreamlike, drowsy, and knowing
Delta	0.1– 4 Hz **If you need to edit the image, please use the original: 326336_0_En_370-1_Fige_HTML.gif**	Deep, dreamless sleep, trance, and unconscious

Brain-Computer Interface (BCI)

"Brain-computer interface is a method of communication based on neural activity generated by the brain and is independent of its normal output pathways of peripheral nerves and muscles" (Vallabhaneni et al. *2005*). BCIs are developed by the research community with some applications in mind to the generation of new assistive devices (Rao and Scherer *2010*). Brain-computer interface technology is a powerful communication tool for both users and systems. "The BCI has the capacity to access brain activities and impart relevant information on the emotional status of the user" (AbuHashish *2015*). There is no need for any external devices or muscle involvement to issue instructions and complete the communication (Bi et al. *2013*). Normal individuals have been targeted in most recent studies by exploring the use of BCIs as an input device and exploring the generation of hands-free applications (van Erp et al. *2012*).

BCI Types

The BCI can be separated into invasive, partially invasive, and noninvasive types (Abhang et al. *2016*). In invasive BCI, recording the signals occurs when electrodes enter the brain tissue. This is a permanent basis method, which buries electrodes within the brain. Partially invasive BCI is a process in which electrodes are placed inside of the skull but rest outside the brain rather than within the gray matter above the brain's surface. A good example for partially invasive BCI is electrocorticography (ECoG). ECoG is a type of monitoring that uses electrodes placed directly on the bare surface of the brain to record brainwaves from the cerebral cortex (Palmini *2006*). In noninvasive type of BCI, no surgery is needed. Instead, the sensors or electrodes are placed over the head (via a hat, belt, patch, or a headset) to measure electroencephalography (EEG), which reads the rhythm of brain activities (*Mayoclinicstaff Electromyography (EMG)*). There are many brain devices that are used to capture brain activities. These devices are brain controllers, which are very common technologies in the BCI area that can read the electrical brain functions (Abuhashish et al. *2015b*). The following image (Fig. *3*) shows the different layers of the brain and where the signal is taken from by three different methods such as EEG, ECoG, and implant.

Fig. 3

The way that BCI captures the signals from the human brain (*Mayoclinicstaff Electromyography (EMG)*)

BCI System Process

A BCI is a system that can distinguish a definite set of forms in brain signals following five sequential stages (Fig. 4): signal acquisition, preprocessing or signal enhancement, feature extraction, classification, and the application interface (Khalid et al. *2009*). You can see in Fig. 4 that the first part of BCI process starts with acquiring the signals from the brain and goes to the next section, which has three subsections for signal processing to make the signal ready to use in different applications and for different purposes.

Fig. 4

Brain-computer interface process

Signal acquisition is a considerable challenge in the field of BCI. Some methods focus on EEG signals; however, other methods exist that can capture neurological activity. End use is a factor that is intended by the designer which filters out which method you should use for capturing specific signals (Major and Conrad *2014*). Different methods for signal acquisition have been studied. There are two general classes of brain acquisition methods, which are invasive and non-invasive (Fig. 5). Each method is using different types of BCI devices.

Fig. 5

Brain signal acquisition's methods

After signal acquisition part, signals are going to be preprocessed. Signal preprocessing is also called signal enhancement (Norani et al. *2010*). In general, the acquired brain signals are unclear by noise and artifacts. The artifacts are eye blinks, eye movements, and heartbeat. In addition to these, muscular movements and power line intrusions are also mixed with brain signals (Bin et al. *2009*). A couple of different methods are used for artifact removal which "the most frequently used methods are Common Average Referencing (CAR), Surface Laplacian (SL), Common Spatial Patterns (CSP), Independent Component Analysis (ICA), Principal Component Analysis (PCA) and Adaptive Filtering" (Lee et al. *2010*). Overall, these techniques have specific purposes that could match each objective of experiments conducted (Mallick & Kapgate, *2015*).

After preprocessing and filtering, the EEG signals will pass through feature extraction process and select particular features by some feature selection methods. Some researcher used a hybrid BSS-SVM system to extract the movement-related features from the EEGs (Peterson et al. *2005*). In most existing BCI, this identification relies on a classification algorithm. Using classification algorithms is the most popular tactic for this purpose. These procedures are used to identify "patterns" of brain activity (McFarland et al. *2006*).

Classification algorithms divided into five different categories: linear classifiers, neural networks, nonlinear Bayesian classifiers, nearest neighbor classifier, and combinations of classifiers (Lotte et al. *2007*). BCI has many applications, especially for disabled persons. It reads the signals generated by the brain and translates them into activities and commands that can control the computers (Lotte *2006*). Figure 6 shows the different types of BCI applications.
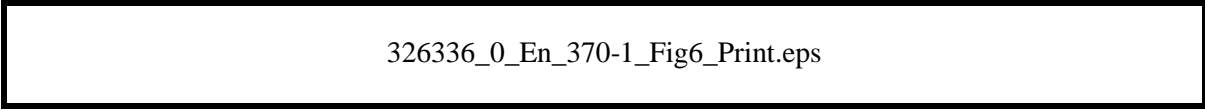
```
326336_0_En_370-1_Fig6_Print.eps
```

Fig. 6
BCI application fields

BCI Security Authentication Using EEG Signals

As the authors mentioned before, a couple of different ways are there which are designed for acquiring the brain activities noninvasively, including magnetoencephalography (MEG), functional magnetic resonance imaging (fMRI), positron emission tomography (PET), near-infrared spectroscopy (NIRS), and electroencephalography (EEG). In comparison to other methods, EEG is a noninvasive method, which is not very expensive and allows recording the signals passively. EEG-based user authentication systems are currently popular in BCI security and authentication applications. Recently, scientists and researchers have been doing many attempts to observing the pattern uniqueness of the brain signal. Several different methods have been used to analyze EEG signals. In regard to the recent progression of EEG signal acquisition devices, the capability of providing better results is going higher, and these processes are getting simpler. The authors are going to review a couple of different tactics of EEG capturing methods to acquire better accuracy and check the applicability of using signal authentication purposes. There are four different studies in this research area that were more successful and reported better accuracy in their experiences (Jayarathne et al. *2017*) which are linear discriminant analysis (LDA), cosine similarity → LDA, power spectral density (PSD) and spectral coherence (COH) → Mahalanobis distance and match-score fusion, and event-related potentials (ERP). These studies used different tasks, extracted features, and classifiers for doing their experiments to get higher accuracy rates of brainwaves to use them for authentication purposes. Besides the studies mentioned above, Table 8 summarizes some other studies with achieved accuracy and other characteristics. Generally, accuracy of each system depends highly on these aspects.**Table 8**
Summary of various studies (in decreasing order of accuracy) (Jayarathne et al. *2017*)

Author(s)	Channels	No. of subjects	Task	Derived or extracted feature	Classifier	Avg. accuracy

Rui-Blondet et al.	3	50	Visual simulation of 400 images	Event-related potentials (ERP)	Normalized cross-correlation	100%
La Rocca et al.	64	108	Relaxation with opened eyes and closed eyes	Power spectral density (PSD), spectral coherence (COH)	Mahalanobis distance-based classifier and match-score fusion	100%
Chen et al.	16	29	Rapid serial visual presentation (RSVP)	Point-biserial correlation coefficients, Fisher's transformation	Linear discriminant analysis (LDA)	100%
Palaniappan	6	6	5 tasks: relaxation, math activity, geometric figur	Auto-regressive coefficients (AR), spectral power (SP), inter-	LDA	100%

			e rotation, mental letter composition, visual counting	hemispheric power differences (IHPD), inter-hemispheric linear complexity (IHLC)		
Ashby et al.	14	5	4 tasks: relaxation, limb movement, geometric figure rotation, visual counting	AR, SP, IHPD, IHLC, PSD	Support vector machine (SVM)	100%
Chuang et al.	1	15	7 tasks: breathing, simulated finger movement, sport activity, singing/passage recitation, audio	Cosine similarity of the vector representation	k-Nearest neighbor (k-NN)	99%

			listening, color identification, and pass-thought			
Palaniappan	61	20	Drawing of common objects as visual simulation	Multiple signal classification (MUSIC)	k-NN, Elman neural network (ENN)	98%
Riera et al.	4	–	Relaxation	AR, fast Fourier transform (FFT), mutual information, coherence, cross-correlation (EEG and ECG data)	Fisher discriminant analysis (FDA)	98%
Jayarathne et al.	14	12	Imagining four-digit number	Common spatial patter	LDA	97%

			as cognitive task	ns (CSP)		
Liew et al.	8	10	Apprehension of images as visual simulation	Coherence, cross-correlation, mean amplitude	Fuzzy-rough nearest neighbor (FRNN)	92%
Yeom et al.	18	10	Apprehension of images of faces including self-face as visual simulation	Difference of average signals, positive/negative peaks at specific latencies	Nonlinear SVM classifier	86.1%

Discussion

Recent biometric user authentication techniques have some problems and limitations. To cover the recent biometric limitations, we need a new biometric brainwave-based authentication, which is another technique in the extensive range of authentication systems. There are many researches about brain signal patterns and using them as a person authentication. Electroencephalogram (EEG) signals are the most popular method in this process. A couple of different approaches are presented in this way to capture EEG signals and classify them with different classification methods to find the unique signals and use them as an authentication method with more accuracy.

Chen et al. (*2016*) proposed a system within authentication, which is centered on rapid serial visual presentation (RSVP) stimulus. A brain amplifier was used to obtain EEG signals and linear discriminant analysis (LDA) to classify them. A specific association constant calculated the important features. According to the author's notation, a password can be hidden effectively in certain compulsive situations.

Chuang et al. (*2013*) presented a new approach which used the MindWave to obtain data. Seven tasks were executed, including sports activity, breathing, audio listing, simulation of finger movement, color, reciting and identifying music with singing, and pass-thoughts. The classification process is done with the k-nearest neighbor (k- NN) algorithm. The most accurate strategies were for color, audio, and sport. The most difficult one was for the pass-thought task according to the results of the questionnaire that determined user-friendliness with different tasks. Breathing, audio, and color were the straightforward tasks.

La Rocca et al. (*2014*) presented an approach centered around connectivity within EEG spectral coherence. In this method, data samples were gathered from 108 participants during open resting and closed eyes positions. EEG data was captured using a system consisting of 64 different channels with a rate of 160 Hz. Data was filtered to 50 Hz via a low-pass anti-aliasing filter. Spectral coherence (COH) and power spectral density (PSD) analysis techniques were used to extract mental features. To calculate uniqueness, two different algorithms were used separately in this process which were Mahalanobis classifiers that were based on distance and match-score fusion system. This technique is strong and very accurate for user identification. The performance of classification has the possibility of not functioning properly if this classification was used for a larger group of users on traditional hardware and it is less than 100%.

Ruiz-Blondet et al. (*2016*) presented a protocol known as CEREBRE with a band-pass filtering between 1 and 55 Hz, and based on normalized cross-correlation, a simple discriminant function was used for classification. The nominal (four categories, three channels) classifier showed the highest accuracy when all the patterns were used, but both maximum and minimum classifiers showed 100% accuracy. The results presented that the most accurate was for the stimulus oddball and food. The resting pattern had a reduced performance in terms of classification. Authentication centered on a memory-evoking task (also known as "pass-thoughts" in other studies) (Thorpe et al. *2005*) also showed weak results; this is due to the inconstant time that was consumed to allow thinking. According to the limitations of the methods which have been presented in the published papers and researches, the authors need better techniques like using different tasks and user strategies to acquire brain signals, better methods for preprocessing and feature extraction, and better classifiers to find the unique brain signal and use it as a new biometric authentication.

Conclusion

In the near future, biometric authentication methods will be the most useful methods for devices and applications for security because of the usability and security level and they are easier to use. However, there are some disadvantages for some methods. Brainwave is another human biometrics. There were some experiments using brain signals as an authentication method, which in some methods high accuracy is acquired. However, they had some limitations, which can be improved in the future.

Brainwaves are another human biometric that could be the most secure biometric technique. In comparison with other biometric techniques in terms of security, the human brain signal has a couple of important advantages. It is the only biometric that is changeable, it is not visible to duplicate and does not have shoulder surfing problem, and it is more useful for disabled people in which a good example would be the famous scientist Stephen Hawking who was using a kind of brain-computer interface technology.

References

Abhang, P.A., Gawali, B.W., Mehrotra, S.C.: Introduction to EEG and Speech-Based Emotion Recognition. Academic, Amsterdam (2016)

AbuHashish, F.A.M.: Classification technique for human emotion in virtual reality using game-based brain computer interface. Doctoral dissertation, Universiti Teknologi Malaysia (2015)

Abuhashish, F.A., Sunar, M.S., Kolivand, H., Mohamed, F., Mohamad, D.B.: Feature extracted classifiers based on eeg signals: a survey. Life Sci. J. **11**(4), 364, Malaysia (2014)

Abuhashish, F.A.M., Kolivand, H., Shahrizal, M.: Framework of controlling 3D virtual human emotional walking using BCI. Jurnal Teknologi, 75(4), Malaysia (2015)

Abuhashish, F.A., Zraqou, J., Alkhodour, W., Sunar, M.S., Kolivand, H.: Emotion interaction with virtual reality using hybrid emotion classification technique toward brain signals. Int. J. Comput. Sci. Inf. Technol. **7**(2), 159 (2015b)

Agrafioti, F., Bui, F.M., Hatzinakos, D.: Medical biometrics: the perils of ignoring time dependency. In: Proc. IEEE 3rd Int. Conf. Biometrics, Theory, Appl, Syst, pp. 1–6. Washington DC, USA (2009)

Bi, L., Fan, X.A., Liu, Y.: Eeg-based brain-controlled mobile robots: a survey. IEEE Trans. Hum-Mach Syst. **43**(2), 161–176 (2013)
CrossRef

Bin, G., Gao, X., Yan, Z., Hong, B., Gao, S.: An online multi-channel SSVEP-based brain–computer interface using a canonical correlation analysis method. J. Neural Eng. **6**(4), 046002 (2009)
CrossRef

Biometrictoday: 25 advantages and disadvantages of iris recognition. Available at: https://biometrictoday.com/25-advantages-disadvantages-iris-recognition. Last accessed 29 June 2018

Catarino, A., Churches, O., Baron-Cohen, S., Andrade, A., Ring, H.: Atypical eeg complexity in autism spectrum conditions: a multiscale entropy analysis. Clin. Neurophysiol. **122**(12), 2375–2383 (2011)
CrossRef

Chen, Y., Atnafu, A.D., Schlattner, I., Weldtsadik, W.T., Roh, M.C., Kim, H.J., Lee, S.W., Blankertz, B., Fazli, S.: A high-security eeg-based login system with rsvp stimuli and dry electrodes. IEEE Trans. Inf. Forensic Secur. **11**(12), 2635–2647 (2016)
CrossRef

Choraś, R.S.: Retina recognition for biometrics. In: Digital Information Management, ICDIM, 2012 Seventh International Conference, pp. 177–180. IEEE, Macau, China (2012)

Chuang, J., Nguyen, H., Wang, C., Johnson, B.: I think, therefore I am: usability and security of authentication using brainwaves. In: International Conference on Financial Cryptography and Data Security, pp. 1–16. Springer, Berlin (2013)

Darril.: https://blogs.getcertifiedgetahead.com/identification-authentication-authorization. Last accessed 24 June 2018

DeBow, B., Syed, K.: 802.11 wireless network end-user authentication using common access cards. In: Military Communications Conference 2006, MILCOM2006, pp. 1–5. IEEE Washington DC, USA (2016)

Erden, M.: Advantages and Disadvantages of Biometric Authentication. http://www.sestek.com/2016/11/advantages-disadvantages-biometric-authentication. Last accessed 15 June 2018

Faundez-Zanuy, M.: Biometric security technology. IEEE Aerosp. Electron. Syst. Mag. **21**(6), 15–26 (2006)
CrossRef

Imotion EEG packet guide.: https://imotions.com/wp-content/uploads/Guides/iMotions_Guide_EEG_PocketGuide_2016.pdf. Last accessed 3 July 2018

Jafri, R., Arabnia, H.R.: A survey of face recognition techniques. Jips. **5**(2), 41–68 (2009)

Jain, A., Bolle, R., Pankanti, S.: Biometrics: Personal Identification in Networked Society. Kluwer Academic, Norwell (1999)
CrossRef

Jatin, C.: Retina scan: eye on security. https://www.inteligentcomp.com/2012/10/all-about-retina-scan.html. Last accessed 29 June 2018

Jayarathne, I., Cohen, M., Amarakeerthi, S.: Survey of EEG-based biometric authentication. In: Awareness Science and Technology, iCAST, 2017 IEEE 8th International Conference, pp. 324–329. IEEE, Taichung, Taiwan (2017)

Khalid, M.B., Rao, N.I., Rizwan-i-Haque, I., Munir, S., Tahir, F.: Towards a brain computer interface using wavelet transform with averaged and time segmented adapted wavelets. In: Computer, Control and Communication, 2009. ic4 2009. 2nd International Conference, pp. 1–4. IEEE Karachi, Pakistan (2009)

Kittler, J., Ballette, M., Czyz, J., Roli, F., Vandendorpe, L.: Enhancing the performance of personal identity authentication systems by fusion of face verification experts. In: Multimedia and Expo, 2002. ICME'2. Proceedings. 2002 IEEE International Conference, vol. 2, pp. 581–584. IEEE, Lausanne, Switzerland (2002)

Kodituwakku, S.R.: Biometric authentication: a review. Int. J. Trend Res. Dev. **2**(4), 2394–9333 (2015)

Korde, K.S., Paikrao, P.L.: Analysis of EEG signals and biomedical changes due to meditation on brain: a review. Analysis 5(01), 603–606 (2018)

Kute, A., Kumar, V.: Fingerprint recognition system: A review. International Journal of Electrical, Electronics and Computer Engineering, 3(2), 61. (2014)

La Rocca, D., Campisi, P., Vegso, B., Cserti, P., Kozmann, G., Babiloni, F., Fallani, F.D.V.: Human brain distinctiveness based on EEG spectral coherence connectivity. IEEE Trans. Biomed. Eng. **61**(9), 2406–2412 (2014)
CrossRef

Le, C., Jain, R.: A Survey of Biometrics Security Systems. EEUU. Washington University in St. Louis (2009)

Lee, P.L., Sie, J.J., Liu, Y.J., Wu, C.H., Lee, M.H., Shu, C.H., Li, P.H., Sun, C.W., Shyu, K.K.: An ssvep-actuated brain computer interface using phase-tagged flickering sequences: a cursor system. Ann. Biomed. Eng. **38**(7), 2383–2397 (2010)
CrossRef

Lotte, F.: The use of fuzzy inference systems for classification in EEG-based brain-computer interfaces. In: 3rd International Brain-Computer Interfaces Workshop and Training Course (2006)

Lotte, F., Congedo, M., Lécuyer, A., Lamarche, F., Arnaldi, B.: A review of classification algorithms for EEG-based brain–computer interfaces. J. Neural Eng. **4**(2), R1 (2007)
CrossRef

Major, T.C., Conrad, J.M.: A survey of brain computer interfaces and their applications. In: SOUTHEASTCON 2014, IEEE, pp. 1–8. IEEE (2014)

Mallick, A., Kapgate, D.: A review on signal pre-processing techniques in brain computer interface. Int. J. Comput. Technol. **2**(4), 130–134 (2015)

Margaret, R.. https://searchsecurity.techtarget.com/definition/authentication. Last accessed 24 June 2018

Margaret, R.: Facial recognition. https://searchenterpriseai.techtarget.com/definition/facial-recognition. Last accessed 29 June 2018

Masupha, L., Zuva, T., Ngwira, S., Esan, O.: Face recognition techniques, their advantages, disadvantages and performance evaluation. In: Computing, Communication and Security ICCCS, 2015 International Conference, pp. 1–5. IEEE, Pamplemousses, Mauritius (2015)

Mayoclinicstaff Electromyography (EMG). https://www.mayoclinic.org/tests-procedures/emg/about/pac-20393913. Last accessed 5 July 2018

McFarland, D.J., Anderson, C.W., Muller, K.R., Schlogl, A., Krusienski, D.J.: Bci meeting 2005-workshop on bci signal processing: feature extraction and translation. IEEE Trans. Neural Syst. Rehabil. Eng. **14**(2), 135–138 (2006)
CrossRef

Millet, D.: The origins of EEG. In: 7th Annual Meeting of the International Society for the History of the Neurosciences, ISHN (2002)

Neustadter, E., Mathiak, K., Turetsky, BI.: EEG and MEG probes of schizophrenia pathophysiology. In: The Neurobiology of Schizophrenia, pp. 213–236 (2016)
CrossRef

Niedermeyer, E., da Silva, F.L.: Electroencephalography: Basic Principles, Clinical Applications, and Related Fields. Lippincott Williams & Wilkins (2005)

Norani, N.M., Mansor, W., Khuan, L.Y.: A review of signal processing in brain computer interface system. In: Biomedical Engineering and Sciences, IECBES, 2010 IEEE EMBS Conference, pp. 443–449. IEEE, Kuala Lumpur, Malaysia (2010)

Palmini, A.: The concept of the epileptogenic zone: a modern look at Penfield and Jasper's views on the role of interictal spikes. Epileptic Disord. **8**(2), 10–15 (2006)

Peterson, D.A., Knight, J.N., Kirby, M.J., Anderson, C.W., Thaut, M.H.: Feature selection and blind source separation in an eeg-based brain-computer interface. EURASIP J. Adv. Sig. Process. **2005**(19), 218613 (2005)
CrossRef

Prasanna, S.R.M., Sahoo, S.K., Choubisa, T.: Multimodal biometric person authentication: a review. IETE Tech. Rev. **29**, 54–75 (2012)
CrossRef

Rao, R.P., Scherer, R.: Brain-computer interfacing [in the spotlight]. IEEE Signal Process. Mag. **27**(4), 152–150 (2010)
CrossRef

Roux, F., Uhlhaas, P.J.: Working memory and neural oscillations: alpha–gamma versus theta–gamma codes for distinct wm information. Trends Cogn. Sci. **18**(1), 16–25 (2014)
CrossRef

Ruiz-Blondet, M.V., Zhanpeng, J., Sarah, L.: Cerebre: a novel method for very high accuracy event-related potential biometric identification. IEEE Trans. Inf. Forensic Secur. **11**(7), 1618–1629 (2016)
CrossRef

Shekar, B.H., Bhat, S.S.: Steerable riesz wavelet based approach for iris recognition. In: Pattern Recognition, ACPR, 2015 3rd IAPR Asian Conference, pp. 431–436. IEEE, Kuala Lumpur, Malaysia (2015)

Tarun, A.: Fingerprint Identification. https://www.elprocus.com/fingerprint-identification. Last accessed 29 June 2018

Thorpe, J., van Oorschot, P.C., Somayaji, A.: Pass-thoughts: authenticating with our minds. In: Proceedings of the 2005 Workshop on New Security Paradigms pp. 45–56. ACM (2005)

Vallabhaneni, A., Wang, T., He, B.: Brain-computer interface. In: He B. (eds) Neural Engineering. Bioelectric Engineering pp. 85–121. Springer, Boston (2005)

van Erp, J., Lotte, F., Tangermann, M.: Brain-computer interfaces: beyond medical applications. Computer. **45**(4), 26–34 (2012)
CrossRef

Vangie, B.: (n.d.). https://www.webopdia.com/TERM/R/rsa_secure_id.html. Last accessed 24 June 2018

Wayman, J., Jain, A., Maltoni, D., Maio, D.: An introduction to biometric authentication systems. In: Biometric Systems, pp. 1–20. Springer, London (2005)
CrossRef