

METHOD FOR CONTINUOUSLY CONTROLLING ACCESS TO A RESOURCE AND ASSOCIATED DEVICES

The present invention relates to a method for continuously authenticating access to a resource. Same further relates to an authentication system, a computer program product and a readable data storage medium involved in the implementation of such an authentication method.

In the context of a site or equipment with controlled access, it is necessary to be able to ensure with the greatest possible security that the individual requesting to enter the site or to use the equipment is indeed an individual authorized to perform such action.

To this end, it is known to grant access by control of a biometric characteristic such as a fingerprint. It is necessary and sufficient for the individual requesting access to place his/her finger on a fingerprint acquisition sensor and for the access control device to verify that the fingerprint corresponds to the fingerprint of authorized personnel.

However, malicious individuals can stealthily detect fingerprints or force authorized personnel to put their finger on the sensor to gain access to the site or hardware.

There is thus a need for a method of controlling access to a resource that is more secure while remaining easy to implement.

To this end, the description describes a method for continuously controlling access to a resource, the method comprising:

- an initial phase of authentication, the initial phase including a step of:
 - acquisition of a signal relative to the activity of at least one region of the brain of an individual requesting access to the resource, to obtain an acquired signal, the acquisition step being implemented by an acquisition device (16) for the brain activity,
 - extraction of a predefined biomarker of the identity of the individual from the acquired signal, to obtain an extracted biomarker,
 - comparison between the extracted biomarker and at least one authentication biomarker, the authentication biomarkers being biomarkers of at least one individual having access authorization to the resource, to obtain a comparison result,
 - provision of access when the comparison result corresponds to an authentication of the individual requesting access as an individual having an authorization of access to the resource,
- a phase of checking the validity of the initial authentication of the individual requesting access, the control phase comprising a step of:

- measurement of a signal by the acquisition device, to obtain a measured signal,
- application of at least one criterion on the measured signal to determine whether or not each criterion is met, each criterion being different from the comparison made during the initial phase,
- implementation of a series of predefined actions, the series of actions comprising:
 - when each criterion is met, maintaining the access and a new implementation of the steps of the control phase, and
 - when at least one criterion is not met, the cessation of access to the resource.

According to particular embodiments, the method of continuous control has one or a plurality of the following features, taken individually or according to all technically possible combinations:

- a criterion used in the application step is a criterion of the capacity of the acquisition device to acquire said signal relative to the activity of at least one region of the brain of the individual requesting access to the resource.
- the acquisition device is an electroencephalograph with electroencephalography sensors and wherein:
 - during the measurement step, the measured signal is a signal relative to the activity of at least one region of the brain of the individual requesting access to the resource, and
 - during the application step, the capacity criterion corresponds to a comparison between the quality value of the measured signal and a predetermined quality threshold.
- the acquisition device is an electroencephalograph with electroencephalography sensors and wherein:
 - during the measurement step, the measured signal is a signal relative to the activity of at least one region of the brain of the individual requesting access to the resource, and
 - during the application step, the capacity criterion corresponds to a comparison between the amplitude of the measured signal and a predetermined amplitude threshold for a plurality of predefined frequencies.
- a criterion used during the application step is a criterion of mental state of the individual requesting access to the resource to access the resource.

- during the measurement step, the measured signal is a signal relative to the activity of at least one brain region of the individual requesting access to the resource, and during the application step, biomarkers are extracted from the measured signal and the mental state criterion corresponds to a comparison between the biomarkers extracted from the individual requesting access to the resource and threshold values.

- the initial phase further includes a step of testing the liveness of the individual by measuring the brain response to predefined excitations, to determine whether the individual requesting access is actually present, and, during the provision step, access is only provided if the individual requesting access is determined to be present.

The description also describes a system for continuously controlling access to a resource, the control system comprising:

- a device for the acquisition of brain activity, the acquisition device being suitable for:

- acquiring, during an initial authentication phase, a signal relative to the activity of at least one region of the brain of an individual requesting access to the resource, to obtain an acquired signal,

- measuring a signal, during a phase of checking the validity of the initial authentication of the individual requesting access, to obtain a measured signal,

- a controller apt:

- during the initial phase of authentication:

- to extract a predefined biomarker of the identity of the individual from the acquired signal, to obtain an extracted biomarker,

- to compare the extracted biomarker and at least one authentication biomarker, the authentication biomarkers being the biomarkers of at least one individual having an authorization of access to the resource, to obtain a comparison result,

- to provide access when the comparison result corresponds to an authentication of the individual requesting access as an individual with access authorization to the resource,

- during the control phase:

- to apply at least one criterion on the measured signal to determine whether each criterion is met or not, each criterion being different from the comparison made during the initial phase,

- to implement a series of predefined actions, the series of actions comprising:

- when each criterion is met, maintaining the access and a new implementation of the steps of the control phase, and
- when at least one criterion is not met, the cessation of access to the resource.

The description further relates to a computer program product comprising instructions which, when the program is executed by a computer, lead the computer to implement the steps of extraction, comparison, provision, application and implementation according to a control method as described hereinabove.

The description further relates to a computer-readable data storage medium on which is stored a computer program product such as described hereinabove.

In the present description, the expression "suitable for" means equally well "apt to" or "configured for".

The features and advantages of the invention will appear upon reading the following description, given only as an example, but not limited to, and making reference to the enclosed drawings, wherein:

- Figure 1 is a schematic representation of an example of a system for continuously controlling the access of an individual to a resource, and
- Figure 2 is a schematic representation of a part of the control system.

A system 10 for continuously controlling access to a resource 12 is shown in Figure 1.

The control system 10 is apt to control the access of an individual 14 to the resource 12.

The control system 10 is thereby apt to verify that the individual 14 does indeed have an authorization to access the resource 12.

Herein, such a check is carried out continuously.

"Continuous" means in the present context that access is not permanent. Access is checked a plurality of times and preferably constantly.

For example, after a first check of access, a real-time detection of disconnection of sensors is implemented to detect any variation (change of identity or movement of the authenticated individual). In such a case, the check is considered to be ongoing.

The resource 12 is any type of restricted-access element.

For example, a computer, files, a machine or a room may be subject to controlled access, i.e. only certain individuals have the authorization of access. Other individuals are not allowed access to the controlled-access elements.

According to the example shown in Figure 1, the resource 12 is a computer.

The control system 10 includes an acquisition device 16 for acquiring brain activity, a controller 18 and a human-machine interface 20.

5 The acquisition device 16 is a device for measuring brain activity, i.e. the activity of at least one region (or zone) of the brain.

Such an acquisition device 16 may be an electroencephalograph or a functional imaging device, such as an ultrasound imager or an imager suitable for implementing a magnetic resonance imaging technique (such technique being more often referred to by the corresponding acronym of MRI).

10 Hereinafter and in accordance with the example of Figure 1, it is assumed without loss of generality that the acquisition device 16 is an electroencephalograph 16.

The electroencephalograph 16 is a device for obtaining electroencephalography signals. Such signals are often referred to as EEG signals with reference to the corresponding abbreviation.

15 As can be seen in Figure 1, the electroencephalograph 16 includes a headset 22 and electroencephalography sensors 24.

The headset 22 is intended to be positioned on the head of the individual 14.

The sensors 24 are suitable for measuring the electrical activity of a region of the brain of the individual 14.

20 The sensors 24 are e.g. electrodes.

The sensors 24 are positioned at a plurality of different locations on the head of the individual 14.

The controller 18 is a physical entity, such as a computer.

25 According to a first example, the controller 18 comprises a processor 26, a memory 28 and a reader 30 for a data storage medium.

The controller 18 is intended to interact with a computer program product comprising a data storage medium readable by the reader 30 of the controller 18.

30 The readable data storage medium of the computer program product is e.g. a medium suitable for storing electronic instructions and apt to be coupled to a bus of a computer system.

As an example, the computer-readable data storage medium is a USB stick, a diskette or a floppy disk, an optical disk, a CD-ROM, a magneto-optical disk, a ROM, a RAM, any type of non-volatile memory (e.g. EPROM, EEPROM, FLASH, NVRAM), a magnetic card or an optical card.

35 A computer program containing program instructions is stored on the readable data storage medium.

The computer program can be loaded into the processor 26 and is suitable for leading to the implementation of steps which will be described hereinafter in the description.

According to a second example, the controller is a hardware, such as a Field Programmable Gate Array (FPGA), or a dedicated integrated circuit, such as an ASIC (Application-Specific Integrated Circuit).

In the case shown in Figure 1, the controller 18 is integrated into headset 22.

In a variant, the controller 18 is remote from the headset 22 and communicates with the headset 22 via a wired link or a wireless link such as Bluetooth or WiFi.

According to the example, the human-machine interface 20 is a screen apt to send visual messages to the individual 14.

In a variant or in addition, the human-machine interface 20 comprises a sound reproduction member and the message is a sound signal.

The human-machine interface 20 is e.g. integrated into a portable device 32 (illustrated in Figure 1), such as a smartphone 32. For example, an application is installed on the smartphone 32 that serves for the interaction between the controller 18 and the human-machine interface 20.

In one example, the controller 18 and the human-machine interface 20 are integrated into the same device e.g. a portable device, such as a smartphone.

The operation of the control system 10 is now described with reference to an example of implementation of a method for continuously controlling the access to the resource 12.

The control method aims to control the access of the individual 14 to the resource 12.

In other words, it is a question of checking that the individual 14 requesting access to the resource 12 is an individual who has an authorization of access.

The control method tries to carry out the check continuously.

For this purpose, the method includes two phases: an initial phase of authentication and a phase for checking the validity of the initial authentication.

The initial phase of authentication comprises, according to the example described, an acquisition step, an extraction step, a comparison step and a provision step.

During the acquisition step, the electroencephalograph 16 records, at the scalp, a signal relative to the activity of at least one region of the brain of the individual 14 requesting access to the resource.

The signal related to brain activity corresponds to the electromagnetic oscillations generated by the brains of human beings.

All regions of the brain are subject to such oscillations with variations depending on the region considered.

Also, the regions chosen may vary according to the nature of the check to be carried out.

5 For example, in order to detect the activity of the frontal cortex, it may be chosen to place the electrodes at the frontal region of the head.

At the end of the acquisition step, the control system 10 thereby has an acquired signal.

10 The controller 18 then extracts, during the extraction step, at least one predefined biomarker of the identity of the individual.

By definition, a predefined biomarker of the identity of the individual is a distinctive feature of the acquired signal, which is herein an electroencephalogram.

An example of a predefined biomarker is a spectral characteristic such as the representative rhythm of a brain wave, such as the alpha rhythm or the beta rhythm.

15 The alpha rhythm is a rhythm characterizing the oscillatory cerebral electrical activity in a frequency band grouping together frequencies typically comprised between 7.5 Hertz (Hz) and 14 Hz.

20 Similarly, the beta rhythm characterizes oscillatory brain electrical activity in a frequency band grouping together frequencies typically greater than 15 Hz, and generally less than 30 Hz.

The ratio between the different rhythms, the center frequency of each rhythm, the power of alpha waves, the power of beta waves, the spectral power on a specific frequency band, the magnitude of the electrical activity at a plurality of frequencies are other examples of predefined biomarkers of the identity of the individual.

25 Therefore, the biomarker is herein a brain signature specific to an individual. The uniqueness thereof ensures a good authentication of the individual.

Biomarkers are predefined in the sense that the determination thereof has to allow the comparison step to be carried out.

30 The controller 18 thereby has an extracted biomarker, i.e. a value for the biomarker predefined for the individual 14 requesting access.

During the comparison step, the controller 18 then performs a comparison between the extracted biomarker and at least one authentication biomarker.

35 The authentication biomarkers are the biomarkers of at least one individual who has an authorization to access the resource. The authentication biomarkers are stored in a memory 28 of the controller 18.

Herein, the comparison consists in ensuring that the authentication biomarker and the extracted biomarker are identical within a margin.

The margin is generally the measurement error in the determination of the extracted biomarker.

5 According to one variant, the individual 14 can declare his/her identity prior to the comparison step and the comparison is performed only with the authentication biomarker corresponding to the declared identity.

At the end of the comparison step, the controller 18 thereby has a result of the comparison.

10 The controller 18 then either provides or does not provide access to the resource.

The provision takes place according to the result of the comparison

The controller 18 provides access to the resource only when the comparison result corresponds to an authentication of the individual 14 requesting access as an individual having an authorization of access to the resource.

15 At each of the aforementioned steps, the human-machine interface 20 can display indications intended for the individual 14 trying to identify himself/herself.

For example, the human-machine interface 20 may indicate that the comparison is in progress or whether authentication was successful or not.

20 The control system 10 then implements the phase of checking the validity of the initial authentication.

The above means herein to check that it is always the same individual 14 who uses the resource.

According to the example described, the control phase includes a measurement step, an application step and an implementation step.

25 During the measurement step, the electroencephalograph 16 measures a signal.

During the application step, the controller 18 applies a criterion to the measured signal in order to determine whether the criterion is met or not.

30 According to a first example, the criterion is a criterion of the capacity of the electroencephalograph 16 to acquire said signal relative to the activity of at least one region of the brain of the individual 14 requesting access to the resource 12.

In such an example, the measured signal is a signal representative of the activity of at least one region of the brain of the individual 14 requesting access.

The controller 18 then evaluates the capacity criterion by a comparison between the quality of the acquired signal and a predetermined quality threshold.

Typically, if the quality of the measured signal falls below a predetermined value, thereof is a sign that the contact between the sensors 24 and the head of the individual 14 is very poor.

5 The quality of the signal is e.g. evaluated by determining the variation in the signal-to-noise ratio.

In a variant or in addition, the controller 18 can use as a capacity criterion a comparison between the amplitude of the signal and a predetermined amplitude threshold for a plurality of predefined frequencies.

10 Typically, if, at all the predefined frequencies, the amplitude of the measured signal is too high, thereof also means that the contact between the sensors 24 and the head of the individual 14 is very poor.

According to a second example, the criterion is a criterion of mental state of the individual 14 requesting access to the resource 12.

15 Typically, an individual does not have the mental capacity to access a resource 12 if they are stressed, lacks vigilance or show signs of fatigue affecting their mental state. Thereof can come either from the individual themselves or from a change in the environment. The mental state is thus herein a criterion evaluating whether the individual 14 is in the same conditions as during the implementation of the initial phase of authentication.

20 To determine the mental state of the individual 14, the measured signal is e.g. a signal relative to the activity of at least one region of the brain of the individual requesting access to the resource 12.

The measured signal is thereby the same signal as the acquired signal but at a subsequent moment.

25 In a variant, if relevant, the measured signal could be a signal coming from other regions.

During the application step, the controller 18 extracts from the measured signal, biomarkers of the mental state and the controller 18 compares the extracted biomarkers with threshold values.

30 The threshold values are predefined and determined beforehand and are stored in the memory 28 of the controller 18.

According to a third example, the criterion to be met is a set of at least two sub-criteria.

35 According to a particular case of the third example, the two sub-criteria are the criterion of capacity of the electroencephalogram 16 and the criterion of mental state of the individual 14.

At the end of the application step, the control system 10 thereby knows whether the chosen criterion is met or not.

In each case, the criterion is different from the authentication requested in the initial phase. As a result, the check is simpler than obtaining the access.

5 The control system 10 then implements a series of predefined actions which depends on the outcome of the application step.

10 In other words, when the criterion is met, the control system 10 implements a first series of actions whereas, when the criterion is not met, the control system 10 implements a second series of actions, the first series of actions being very different from the second series of actions.

The first series of actions includes maintaining the access and a new implementation of the steps of the control phase.

The time gap with the new implementation is preferably as small as possible, typically one second.

15 According to the example described, the second series of actions includes ceasing the access to the resource.

In such a case, the individual 14 must go through the initial phase steps if he/she wishes to again have access to the resource 12.

20 According to another example, the second series of actions also includes a warning telling the individual 14 that the criterion is not met.

Typically, the human-machine interface 20 displays a message indicating that the control system 10 will prohibit access within a few seconds if the contact between the sensors 24 and the head of the individual 14 is not improved in the meantime.

25 The control method that has just been described has the advantage of a certain universality insofar as any live person generates unique brain signals.

Furthermore, the level of security imparted by the control method is high.

Indeed, electroencephalography data cannot be detected stealthily and cannot be generated artificially.

30 Thereof limits the possibility of impersonating the individual, unlike e.g. an authentication based on a password or on fingerprints. Stealing electroencephalography data is not possible.

Furthermore, brain signals cannot be extracted without the collaboration of the individual wishing to have access to the resource 12.

35 Thereof prevents the 14 individual from accessing the resource 12 under threat, and thereby a forced extraction of the access.

In addition, the method continuously ensures that the individual 14 accessing the resource 12 is always the same who was priorly authenticated.

Such guarantee is obtained with a good level of security and easier implementation than a periodic check of identity by repetition of the steps of the initial phase.

5 Indeed, the continuous extraction of the cerebral signature of the individual 14 to be identified requires the execution of a task, increases the workload and thereby generates stress in the individual and thereby decreases their productivity.

Moreover, the method does not explicitly involve executing a task after the first authentication, so the method is considered silent.

10 The method thereby makes it possible to perform continuous authentication of the identity of the individual 14 under operational conditions while avoiding a cognitive impact on the workload of the individual 14 since the complete authentication is performed only once.

15 As a result, the method remains quick to implement since only the initial authentication takes more than a few seconds (typically 3 seconds), the rest of the actions performed being completely transparent to the individual 14 requesting the access.

Furthermore, the method can be used to determine potentially dangerous alterations, such as the making of a threat to the individual 14 or the degradation of the mental state of the individual 14, in a reliable and silent manner.

20 If need be, the security level of the control method can be increased.

In particular, it is possible to envisage an embodiment in which the method further includes a procedure called the procedure of *liveness detection*.

25 To this end, according to one example, the initial phase further includes a step of testing the liveness of the individual 14 by measuring the cerebral response to predefined excitations, to determine whether the individual 14 requesting access is awake.

Predefined excitations are random and can correspond to any type of excitations. As an example, same could be a visual or an audible excitation.

Such excitations are called *pings*.

30 In the presence of such excitations, the brain response of the individual 14 shows reproducible patterns. The term *time-locked* is used to refer to such a brain reaction.

The absence of such reproducible patterns in response to excitations is the evidence of a lack of liveness of the individual 14.

For example, thereof can be a sign of using a priorly recorded or synthetically generated signal.

When liveness is tested, during the provision step, the access is only provided if the individual 14 requesting the access is determined to be physically present, i.e. present in front of the control system 10, in particular by wearing the headset 22.

5 The access to the resource 12 is thus only given if, on the one hand, the individual 14 is identified as having an authorization of access to the resource 12 and, on the other hand, the individual 14 requesting the access is determined to be present in front of the control system 10.

The use of such double criterion during the initial authentication phase reinforces the security granted by the implementation of the method of continuous control.

10 A person skilled in the art would understand that the invention is not limited to the examples described in the description and that the embodiments described hereinabove can be combined when such a combination is technically possible.

13
CLAIMS

1. A method for continuously controlling access to a resource (12), the method comprising:

- 5 - an initial phase of authentication, the initial phase including a step of:
- acquisition of a signal relative to the activity of at least one region of the brain of an individual (14) requesting access to the resource (12), to obtain an acquired signal, the acquisition step being implemented by an acquisition device (16) for the brain activity,
 - 10 - extraction of a predefined biomarker of the identity of the individual from the acquired signal, to obtain an extracted biomarker,
 - comparison between the extracted biomarker and at least one authentication biomarker, the authentication biomarkers being biomarkers of at least one individual having access authorization to the resource, to obtain a comparison
 - 15 result,
 - provision of access when the comparison result corresponds to an authentication of the individual (14) requesting access as an individual having an authorization of access to the resource (12),
 - a phase of checking the validity of the initial authentication of the individual (14)
 - 20 requesting access, the control phase comprising a step of:
 - measurement of a signal by the acquisition device (16), to obtain a measured signal,
 - application of at least one criterion on the measured signal to determine whether or not each criterion is met, each criterion being different from the
 - 25 comparison made during the initial phase,
 - implementation of a series of predefined actions, the series of actions comprising:
 - when each criterion is met, maintaining the access and a new implementation of the steps of the control phase, and
 - 30 - when at least one criterion is not met, the cessation of access to the resource (12).

2. The method for continuously controlling according to claim 1, wherein a criterion used in the application step is a criterion of the capacity of the acquisition device (16) to

35 acquire said signal relative to the activity of at least one region of the brain of the individual (14) requesting access to the resource. (12).

3. The method for continuously controlling according to claim 2, wherein the acquisition device (16) is an electroencephalograph having electroencephalography sensors (24) and wherein:

- 5 - during the measurement step, the measured signal is a signal relative to the activity of at least one region of the brain of the individual (14) requesting access to the resource, and
- during the application step, the capacity criterion corresponds to a comparison between the quality value of the measured signal and a predetermined quality
- 10 threshold.

4. The method for continuously controlling according to claim 2, wherein:

- during the measurement step, the measured signal is a signal relative to the activity of at least one region of the brain of the individual (14) requesting access to the
- 15 resource, and
- during the application step, the capacity criterion corresponds to a comparison between the amplitude of the measured signal and a predetermined amplitude threshold for a plurality of predefined frequencies.

20 **5.** The method for continuously controlling according to any of claims 1 to 4, wherein a criterion used in the application step is a criterion of mental state of the individual (14) requesting access to the resource (12).

6. The method for continuously controlling according to claim 5, wherein:

- 25 - during the measurement step, the measured signal is a signal relative to the activity of at least one region of the brain of the individual (14) requesting access to the resource, and
- during the application step, biomarkers are extracted from the measured signal and the criterion of mental state corresponds to a comparison between the biomarkers
- 30 extracted from the individual (14) requesting access to the resource (12) and threshold values.

7. The method for continuously controlling according to any of claims 1 to 6, wherein the initial phase further includes a step of testing the liveness of the individual (14)

35 by measuring the brain response to predefined excitations, to determine whether the

individual (14) requesting access is actually present, and, during the provision step, access is only provided if the individual (14) requesting access is determined to be present.

- 5 8. A control system (10) for continuously controlling access to a resource (12), the control system (10) comprising:
- an acquisition device (16) for the acquisition of brain activity, the acquisition device (16) being suitable for:
 - acquiring, during an initial authentication phase, a signal relative to the activity of at least one region of the brain of an individual (14) requesting access to the resource (12), to obtain an acquired signal,
 - measuring a signal, during a phase of checking the validity of the initial authentication of the individual (14) requesting the access, to obtain a measured signal,
 - a controller apt:
 - during the initial phase of authentication:
 - to extract a predefined biomarker of the identity of the individual from the acquired signal, to obtain an extracted biomarker,
 - to compare the extracted biomarker and at least one authentication biomarker, the authentication biomarkers being the biomarkers of at least one individual having an authorization of access to the resource (12), to obtain a comparison result,
 - to provide access when the comparison result corresponds to an authentication of the individual requesting access as an individual with access authorization to the resource,
 - during the control phase:
 - to apply at least one criterion on the measured signal to determine whether or not each criterion is met, each criterion being different from the comparison made during the initial phase,
 - to implement a series of predefined actions, the series of actions comprising:
 - when each criterion is met, maintaining the access and a new implementation of the steps of the control phase, and
 - when at least one criterion is not met, the cessation of access to the resource (12).

9. A computer program product comprising instructions which, when the program is executed by a computer, lead the computer to implement the steps of extraction, comparison, provision, application and implementation according to a method for continuously controlling according to any one of the claims 1 to 8.

5

10. A computer-readable storage medium having stored thereon the computer program according to claim 9.