(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 March 2020 (19.03.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/053610 A1

(51) International Patent Classification:
G06K 9/00 (2006.01)

(21) International Application Number:
PCT/IB2018/001074

(22) International Filing Date:
14 September 2018 (14.09.2018)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicants: **SOLOVEV, Sergei, Vladimirovich** [RU/RU]; Yegor'yevskiy district, Village Bruski, House 18, Moscow Region 140332 (RU). **TRIFOI, Victor, Mikhaylovich** [MD/MD]; MD, str. Cojocarilor, 18, ap. 16, Chisinau 2001/06 (MD).

(72) Inventor; and
(71) Applicant: **SHARIFOV, Sabukhi Knyaz-ogly** [RU/RU]; Balashikha, Ob'edineniya st., 9/28 ap. 73, Moscow Region 143905 (RU).

(74) Agent: **SAVELYEV, Alexander, Viktorovich**; of. 43, 1 building, 19 House, Nezhinskaya street, Moscow, 119517 (RU).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

Published:
— *with international search report (Art. 21(3))*

(54) **Title:** A METHOD FOR AUTOMATIC CONTACTLESS AUTHENTICATION

(57) **Abstract:** A method for automatic contactless authentication including remote irradiating a biological object with a probing radio signal, receipting the signal reflected from the biological object, fixation an individual unique time-stable electromagnetic profile of the object, and identification of the biological object based on this profile. Also in the method fixation an individual unique time-stable electromagnetic profile of biological object is carried out: generating a probing radio signal; whereby the probing signal is multifrequency and consists of at least two radio signals in the microwave and extremely high- frequency bands; whereby the radio signals in the microwave and extremely high-frequency bands are pre-modulated; radiating of with the generated probing signal; information processing of the reflected signal. The probing radio signal may be modulated by a white noise signal or by a binary pulse sequence with a random order of codes corresponding to "zero" or "one". A feedback is closed between the reflected signal and the probing signal; whereby the feedback between reflected and probing signals is closed by means of adaptive tuning of the modulating signal spectrum depending on the reflected signal. In the method frequency of generated probing radio signal lies within the range of 1-300 GHz.

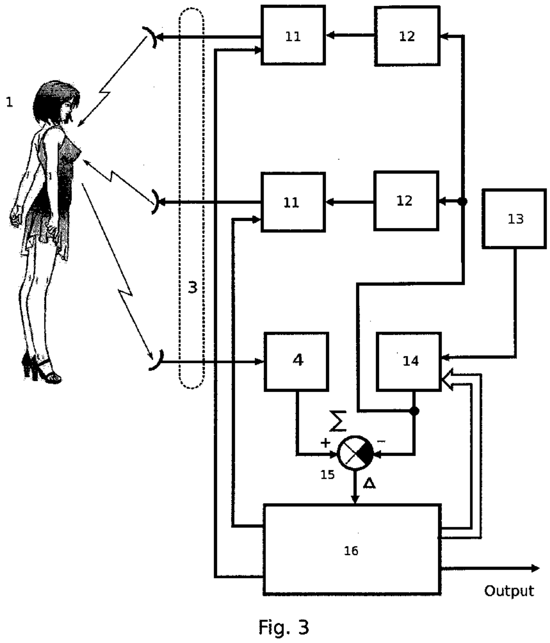

Fig. 3

WO 2020/053610 A1

A method for automatic contactless authentication

FIELD OF THE INVENTION

The invention relates to the field of information security and can be used in any computer systems with biometric authorization for collective or personal use, for example, in electronic commerce systems, electronic banking, electronic document management, etc. for contactless personal identification.

BACKGROUND OF THE INVENTION

User authentication systems are becoming more and more vital due to development of information-oriented society and, respectively, underlying information technologies such as Internet, telecommunications, e-banking, e-shopping, and e-procurement systems. Such systems have become even more necessary in the connection with implementation and global distribution of means for non-cash electronic settlement.

The existing authentication systems, however, require certain actions to be performed by the user, for example, entering and storing passwords, keys, codes, or having a special device able to connection or activation, and so on, which complicate the authentication procedure, that is one of the main disadvantages of such systems. Automatic or semiautomatic systems based on biometric indicators (such as fingerprints, eye iris pattern, hand geometry, voice, heart rhythm, face recognition, etc.) have a low degree of reliability due to ambiguity of recognition, variations in characteristics, strong dependence on indicator presentation quality, weak interference protection and so on. DNA based authentication is extremely complex, time-consuming procedure unable to provide biotechnical system of real-time operator-user interaction.

Known methods and devices can be classified as follows.

First group. Authentication methods based on user-entered ID labels such as passwords, codes, or special devices performing the identification function (such as flash drives, RFID cards, mobile phones, etc.). Typical example of such method is presented in: **WO 2018151480 (A1)** — 2018-08-23. Authentication management method and system. Provided is an authentication management system comprising: a custom credential provider installed in a computing device to support OS account authentication through an alternative authentication technique, which replaces an OS account authentication technique self-supported by an operating system of the computing device; and an authentication management server which is connected to establish communication with the custom credential provider through a communication network, performs user authentication for a user attempting to obtain OS account authentication by using alternative authentication information used in the alternative authentication technique when an attempt to obtain the OS account authentication on the basis of the alternative authentication information has been made, and transfers account authentication information required to perform OS account authentication according to the OS account authentication technique self-supported by the operating system, or a seed value providing a base for creating the account authentication information, to the custom credential provider when the user authentication has succeeded

This group includes, in particular, the auto-identification using an electronic card as described in: **CN 206470768 (U)** — 2017-09-05. Authentication device of built. G06K7/10:

The utility model provides an authentication device of built -in electronic identity card information, it has: memory cell, its electronic identity who is used for the storage to be write in into demonstrate, proves, main control chip, it is equipped with rightly the electronic identity card carries out authentication's authentication processing module, bluetooth radio frequency rf chip, its with main control chip connects, the radio frequency of bluetooth antenna, its with bluetooth radio frequency rf chip connects to be used for communicating with outside bluetooth equipment, two interfaces chip, its with main control chip connects, the induction coil antenna, its with two interfaces chips is connected, and be used for and with the frequency of operation assorted external equipment of induction coil antenna communicates, and communication contact, its with main control chip connects to an external equipment communicates for with support ISOIEC 7816 transfer protocols. Through the utility model discloses an authentication device, the communication interface of the multiple different grade type that can integrate, authentication is carried out to the electronic identity card information that effectively utilizes in the authentication device

Or mobile phone as proposed in: **WO 2017150996 (A1)** — 2017-09-08. A method and a server for authenticating a user with a mobile device. G06F21/31; G06F21/42; H04L29/06; H04W12/06:

The present invention relates to a method for authenticating a user for services, by means of a mobile phone, comprising: receiving, by a server from a service, a request to authenticate a user, assigning an unique access number by the server, presenting the access number from the server to the user via the service, receiving, by the server by means of a terminal device that services the access number, information about a call performed by the user to the access number, the information containing at least the access number and the user's MSISDN, performing, by the server, a basic authentication of the user, comprising at least reading the user's MSISDN and the access number, transferring the result of the basic authentication from the server to the service. The invention also relates to a system authenticating a user, USER, by means of a mobile device

Main disadvantages is that all similar systems, however, require certain actions to be performed by the user, which makes a permanent continuous access right control impossible. Besides, there is a serious difficulty in use of such systems due to necessity to keep in mind keys, passwords, identification numbers and so on. Serious problems can arise due to loss or theft of access devices as well as simplicity of falsification, in other words, low reliability and insufficient security of data protection. The disadvantages include the impossibility of remote contactless monitoring of identification parameters.

Second group. Biometric authentication.

A) Hand recognition: **WO 2018154694** — 2018-08-30. Biometric authentication program, biometric authentication device, and biometric authentication method. 2018-08-30. G06F21/32; G06T7/00:

In the present invention, a biometric image capturing the biometrics of a user is acquired, the orientation of the biometrics in the biometric image is detected on the basis of the acquired biometric image, a template pattern is extracted that matches the orientation detected from a template pattern storage unit in which a plurality of template patterns are stored, feature information from the acquired biometric image is converted to the extracted biometric pattern, and the converted biometric pattern and the extracted template pattern are compared to authenticate the user, whereby correct biometric authentication can be performed even when the orientation of a hand being held up and the orientation of the imaging device differ between the time of registration and the time of authentication of vein data.

US 2018247142 (A1) — 2018-08-30. Biometric authentication device and system. G06F17/30; G06K9/00; G06T7/00; H04L29/06:

A biometric authentication device including a housing, a light source unit that is installed on an upper surface of the housing and includes a light source, and an opening that is provided in the upper surface of the housing and located below the light source, and an imaging unit that is disposed inside the housing is disclosed. In the device, an optical axis of the light source intersects with a longitudinal direction of the housing, and the imaging unit images a user's biometric feature irradiated with an irradiation light from the light source through the opening.

B) Electrocardiographic authentication: **WO 2018152711 (A1)** — 2018-08-30. Electrocardiographic authentication-authentication method therefor. A61B5/0402:

An authentication method for an electrocardiographic authentication-based door control system, comprising: performing feature extraction on a pre-processed electrocardiographic signal by using an autocorrelation transform algorithm, so as to acquire an electrocardiographic autocorrelation sequence; and then performing dimensionality reduction on the electrocardiographic autocorrelation sequence by means of orthogonal polynomial fitted regression, so as to generate a feature template; thereafter selecting and estimating an optimal electrocardiographic feature template so as to acquire the best threshold; and performing user identity authentication on the basis of the optimal electrocardiographic feature template and the best threshold. The authentication method has a high level of security, a high degree of recognition accuracy and less stored authentication information.

RU 2392853 — 2008-09-26. Method of remote breath and heartbeat parametre measurement. A61B 5/08, A61B 5/02, G01S 13/00:

FIELD: medicine. SUBSTANCE: invention refers to methods of examination of physiological functions in living organisms, particularly to radiolocation superbroadband methods of breath and heartbeat parametre diagnostics for patients. Method involves generation of periodic sequence of UHF radio impulses of definite duration, probing radio impulses, reference radio impulses and reference radio impulses phase-shifted by 90 against reference radio impulses. Probing radio impulses are radiated towards examined body part and received in reflected radio impulse intervals. Each reflected radio impulse is correlated with reference radio impulse with further separation of low frequency component of output correlation signals, corresponding to combination of signals caused by examined object movement and signal caused by immobile objects within radiation zone of probing impulses; and each reflected radio impulse is correlated with phase-shifted reference radio impulse with further separation of low frequency component of output correlation signals, corresponding to combination of signals caused by examined object movement and signal caused by immobile objects. Further, presence of signal corresponding to moving object is determined, including signal corresponding to object's chest movement with account of the possible object movement during probing radio impulse radiation, and presence of signal corresponding to chest movement is determined. Signal reflected from immobile objects in probing impulse radiation area is compensated, including substrate surface where the examined object is positioned. Signal corresponding to chest movement is detected, chest movement pattern in time is defined, and decimation and averaging of signal corresponding to chest movement is performed to provide required accuracy of breath and heartbeat parametre measurement. Signal caused by heartbeat is separated from signal corresponding to chest movement, and heartbeat rate is determined. Then signal caused by breath is separated from signal corresponding to chest movement, and breath rate is determined. EFFECT: improved accuracy and reliability of breath and heartbeat parametre measurement due to enhanced phase sensitivity of diagnostics.

This identification method, which is based on individual heart beat patterns, allows to perform continuous remote auto-identification at a short distance, but possesses the low reliability due to large variability of cardiac activity depending on psychophysiological condition of the user. Additional determination of the heart size also does not allow to achieve high reliability for the same reasons as well as possibility of significant change of identification parameters due to a heart disease or even short-term heart seizure or pain.

C) Fingerprint recognition, for example, **WO 03096260 (A2)** — 2003-11-20. Authentication with biometric data. G06K9/00; G06T1/00; G06T7/00; G06K9/00:

The invention relates to an authentication method comprising biometric characteristic data, especially characteristic data taken from finger-prints. According to the invention, the characteristic data is captured at least twice for each authentication request, and a position alteration between successive captures is evaluated and rated.

As well as: **JP 2010198309 (A)** — 2010-09-09. Data processing apparatus with biometric authentication function. G06F21/20; G06F3/041; G06F9/445. **JP 2011095854 (A)** — 2011-05-12. Device with lock. A61B5/117; E05B49/00; G06T1/00. **US 2014043138 (A1)** — 2014-02-13. Key fob with protected biometric sensor. G07C9/00.

Common weakness of fingerprint authentication method consists in low reliability due to the fact that this biometric characteristic can be clogged, damaged or lost. Moreover, it is weakly protected against forgery. The necessity of manual data entry and the complete absence of remoteness are essential disadvantages of this method as well.

D) Voice recognition, **US 10019561 (B1)** — 2018-07-10. Systems and methods for continuous biometric authentication. G06F15/16; G06F17/30; G06F21/32; G06F7/04; G10L17/24; H04L29/06:

Methods and systems for authenticating a user are described. In some embodiments, a series of voice interactions are received from a user during a voiceline session. Each of the voice interactions in the series of voice interaction may be analyzed as each of the voice interactions are received. A confidence level in a verification of an identity of the user may be determined based on the analysis of each of the voice interactions. An access level for the user may be automatically updated based on the confidence level of the verification of the identity of the user after each of the voice interactions is received.

US 10013983 (B1) — 2018-07-03. Selective passive voice authentication. G06K9/00; G10L17/06; G10L17/22; H04L29/06; H04W12/06; H04W12/08; G06Q20/40:

Methods, systems, and apparatus, including computer programs encoded on a computer storage medium, for authenticating a user using a voice biometric program are described. In some embodiments, first voice data from a user device is received. The first voice data can include audio data of a user speaking a first voice command, and the system can determine that the first voice command includes a voice command for which voice recognition can be performed. In response, the system can initiate a passive authentication scheme for selectively enabling access to secure data in response to the first voice command. The passive authentication scheme can provide the first voice data for voice recognition and receive an indication that the user is authenticated based on the voice recognition and, in response, allow access to a back-end system.

Despite the simplicity of these approaches in use, known methods have disadvantage of low recognition reliability due to variability of the voice characteristics, including the dependence on the psychoemotional condition as well as simplicity of falsification or forgery by playing the recorded voice. Another disadvantage again consists in necessity to enter data, i.e. such systems operate only in response to presentation of a voice.

E) Face recognition, **KR 20180087088 (A)** — 2018-08-01. User authentication system using face recognition and biometric authentication card and method thereof. G06F21/32; G06F21/45; G06K9/00; G07C9/00; H04W4/00:

The present invention relates to a system and method for authenticating a user, and more particularly to a system and method for authenticating a user by performing biometric authentication using a face recognition user authentication for recognizing a face of a user walking to a user authentication area, And a biometric authentication security card user authentication for performing user authentication based on the authentication result information upon touching the user authentication means in the user authentication area storing the authentication result information according to the authentication, And a user authentication system using the biometric authentication security card.

In particular, face thermal pattern recognition, **US 2015358557 (A1)** — 2015-12-10. Thermal recognition systems and methods. H04N5/225; H04N5/33:

Various techniques are disclosed for providing object recognition using thermal imaging. Unique thermal features of an object such as a human face can be detected using a thermal imaging module. The thermal imaging module may be included in an authentication system that performs authentication operations for users of a secure system based on the detected thermal features. The thermal features may include a thermal map of a user's face. An object recognition system such as an authentication system may include a non-thermal imaging module that captures non-thermal images of the object. The object recognition system may recognize objects using thermal images and non-thermal images in separate object recognition operations or by combining the thermal and non-thermal images and performing object recognition operations using the combined image. A thermal imaging authentication system may help eliminate user passwords on phones, tablets, computers and/or other secure access systems.

Or, for example, the thermal method of authentication **KR 20150069799 (A)**— 2015-06-24. Method for certifying face and apparatus thereof. G06K9/46.

Known methods demonstrate quite high remoteness (up to tens of meters) and possibility of continuous monitoring, but a low degree of reliability due to complexity of the problem and large ambiguity due to the dependence on the aspect angles. Once more significant disadvantage is weak interference protection, especially in the case of recognition of thermal patterns.

F) Eye iris recognition **KR 20150077179 (A)** — 2015-07-07. Device for photographing an iris and iris authentication device. H04N5/225:

The present invention relates to an apparatus for capturing an iris which is a type of biometric data, capable of acquiring an iris image of a required size when recognizing the iris by filming the iris, which is a subject, by adding a view angle adjusting pipe to a single vision lens in order to acquire a clear iris image, and furthermore capable of acquiring the clear iris image by adding a band pass filter only enabling to penetrate an infrared ray of a certain infrared ray wavelength range and a visible ray of a bluish visible ray wavelength range to a front end of the single vision lens when filming a bluish iris as well as a brownish iris.

CN 108027881 (A) — 2018-05-11. User authentication using multiple capture techniques. G06K9/00; G06K9/20; G06K9/22.

Examples are disclosed herein that relate to user authentication. One example provides a biometric identification system comprising an iris illuminator, an image sensor configured to capture light reflected from irises of a user as a result of those irises being illuminated by the iris illuminator, a drive circuit configured to drive the iris illuminator in a first mode and a second mode that eachcause the irises to be illuminated differently, the first and second modes thereby yielding a first mode output at the image sensor and a second mode output at the image sensor, respectively, and a processor configured to process at least one of the first mode output and the second mode output and, in response to such processing, select one of the first mode and the second mode for use in performing an iris authentication on the user.

Although human eye iris authentication is one of the most accurate biometric methods of auto-identification, known methods suffer from insufficient security due to the fairly easy forgery, for example, using artificial irises. In addition, is has low intrinsic remoteness, since reliable recognition of eye irises is possible only at a distance of at most one or two meters. Also, there is a difficulty with continuous scanning, since the iris-reading sensors can only be narrow-focused, which causes a strong dependence of system performance on user's head rotation or arbitrary movements in general.

Third group. DNA-based authentication. It is usually carried out using a DNA testing of sweat secretions on fingers, vapors of exhaled air, salivary secretions, etc.

US 11065228 — 2005-02-24. Identity verification system with self-authenticating card. G07F7/1008:

The system contains a DNA test unit for obtaining and transmitting applied machine-readable DNA information from a DNA sample; wherein said stored biometric feature includes stored machine-readable DNA information, said applied biometric feature includes said DNA sample and said DNA test unit transmits said applied machine-readable DNA information to said data lock. The identity verification system, wherein said DNA test unit transmits via wireless technology said results of said DNA test to said data lock. The identity-verification system, wherein said DNA test unit is incorporated on a chip in said card substrate card-reading means that includes a data-processing unit for processing data stored on said security card and a DNA test unit with a DNA sample sensor for on-site DNA analysis; and wherein, when a DNA sample is applied to said DNA sample sensor, said DNA test unit performs a DNA test and transmits results of said DNA test to said data lock.

Despite the high accuracy, there are significant drawbacks, namely, high complexity and duration of analysis as well as impossibility of continuous authentication. In addition, remains of DNA code (sweat secretions, hairs, etc.) on surface of the device used to access the personal data (smartphone, tablet, computer, etc.) greatly reduce the data security.

Fourth group. Combined biometric systems,

KR 20070007185 (A) — 2007-01-12. Personal communication apparatus capable of recording transactions secured with biometric data

The method, wherein the receiving element is capable of receiving biometric data from a biometric measurement means, wherein the biometric measurement means comprises fingerprint imaging of one or more human fingers, An image analysis involving image analysis, a human iris image analysis, a tooth imaging, or an ear contour analysis.

WO 2018117398 (A1) — 2007-01-12. Personal communication apparatus capable of recording transactions secured with biometric data

The method, wherein the receiving element is capable of receiving biometric data from a biometric measurement means, wherein the biometric measurement means comprises fingerprint imaging of one or more human fingers, An image analysis involving image analysis, a human iris image analysis, a tooth imaging, or an ear contour analysis.

Such systems and methods increase the reliability of authentication due to increasing a number of recognition factors of different nature by means of combining above mentioned known methods. However, they combine also disadvantages of these known methods whereas total enhancement is insignificant. In most cases, advantages of combined known methods remain not exceed a simple sum of effects from each method used in combination, while sometimes they do not reach such sum. This can be explained by the fact that disadvantages of each individual method do not disappear in their combination, while these disadvantages are enough important. In addition, compiling a combined authentication method from individual known methods, as a rule, essentially complicates both implementation of combined method and the auto-identification procedure itself.

SUMMARY OF THE INVENTION

The object of the invention is to simplify the authentication procedure due to complete automation with excluding of any special user actions and increase reliability of auto-identification due to continuous or pulsed scanning of user's stable biometric data, namely, his or her electromagnetic profile. The object of the invention is to create such procedure that allows to obtain a time-invariant individual electromagnetic profile of any biological object, including a human. Another component of the object of the invention is to significantly improve access security and protection against unauthorized interferences due to the fact that the proposed method yields a user's individual electromagnetic profile, which does not change during life and cannot be counterfeited. Yet another object of the invention is to increase the accuracy of auto-identification and its interference protection by using only modulated low-intensity electromagnetic waves of microwave and extremely high-frequency bands as well as by implementation of multichannel modes. It is yet another object of the invention to solve the problem of improving performance by providing remoteness and possible identification continuity without any special user's actions or use of passwords, so that the authentication procedure can run in silent mode. It is yet another object of the invention to expand the functionality and increase the versatility by making it possible to use the pulse mode for contactless remote personal identification.

To achieve the objects, the method for automatic contactless authentication is proposed. A method for automatic contactless authentication including remote irradiating a biological object with a probing radio signal, receipting the signal reflected from the biological object, fixation an individual unique time-stable electromagnetic profile of the object, and identification of the biological object based on this profile. Also in the method fixation an individual unique time-stable electromagnetic profile of biological object is carried out: generating a probing radio signal; whereby the probing signal is multifrequency and consists of at least two radio signals in the microwave and extremely high-frequency bands; whereby the radio signals in the microwave and extremely high-frequency bands are pre-modulated; radiating of with the generated probing signal; information processing of the reflected signal.

The probing radio signal is modulated by a white noise signal. Also in the method the probing radio signal is modulated by a binary pulse sequence with a random order of codes corresponding to "zero" or "one". A feedback is closed between the reflected signal and the probing signal; whereby the feedback between reflected and probing signals is closed by means of adaptive tuning of the modulating signal spectrum depending on the reflected signal.

Also in the method irradiation of the biological object is low-intensity. and spectrum of biological object irradiation is matched with geometry and electrodynamic parameters (bioelectrical activity, dielectric constant, etc.) of biological object structures.

Also in the method irradiation frequency range is matched with the frequency of acoustoelectric vibrations of the nuclear membranes or irradiation frequency range is matched with the frequency of acoustoelectric vibrations of cell membranes.

Also in the method frequency of generated probing radio signal lies within the range of 1-300 GHz. Also in the method tissues of biological object subjected to irradiation with radio signals in the microwave and extremely high-frequency bands are used as a broadband nonlinear mixer. The information processing is carried out: using an adaptive artificial neural network; b) using a virtual neural network.

Also in the method the information processing of the signal includes fixation of the dynamics of adaptation parameters of the biotechnical system consisting of organism of biological object and a probing device. The information processing of the signal includes time-history analysis of adaptation parameters of the biotechnical system consisting of organism of biological object and a probing device.

Also in the method time-history of adaptation parameters is compared with a reference and an access signal is continuously generated based on results of the comparison.

Also in the method time-history of adaptation parameters is compared with a database in the single-pulse mode and, when matching, the identification parameters are displayed.

BRIEF DESCRIPTION OF DRAWINGS

Fig. 1 shows an enlarged structural scheme for performing the method of automatic contactless authentication with a continuous comparison of currently measured electromagnetic user profile with its initially saved stable individual electromagnetic portrait.

Fig. 2 shows an enlarged structural scheme for performing a method of automatic contactless authentication using a pulse probe signal with a comparison of currently measured electromagnetic user profile with its initially saved stable individual electromagnetic portrait stored in a database.

Fig. 3 shows a detailed flowchart of the proposed method and a scheme of preliminary information processing according to the proposed method in a two-channel embodiment.

Fig. 4 shows a detailed flowchart of the proposed method and a scheme of preliminary information processing according to the proposed method in the multichannel embodiment.

Fig. 5 presents the form of the probing signal.

Fig. 6 presents the modulated signal corresponding to the probing signal in fig. 5 in the form of a random binary sequence.

Fig. 7 depicts dynamics of changes in the error signal and one of the coefficients of a finite-duration impulse response digital filter.

Figs. 8-13 depict changes in the output signal when its spectrum matches the spectrum of a auto-identified user as a biological object, which is shown in background. It is seen that the signal waveform stays virtually unchanged if the spectra mismatch (cp. figures 8, 9, 12, and 13).

Figs. 10-13 show changes in adaptation parameters and partial dynamics of these changes, which is a unique stable electromagnetic profile of the user.

DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION (DETAILED DESCRIPTION)

In all embodiments of the invention, a biological object 1 (for example, a human operator) is irradiated with continuous, single-pulse, or periodically repeated pulse signals with complex modulation and low intensity (E< 1 μV/m) within microwave and extremely high-frequency bands from 1 to 300 GHz, possibly in a multichannel mode, using a radio transmitter 2 and antenna system 3. The human body absorption bands (in the microwave and extremely high-frequency range) were predicted by us theoretically and discovered experimentally [1, 2]. The continuous or pulse signal 4 reflected from the biological object 1 (user) is received and decoded in a real time. Then it is subjected to an adaptive adjustment 5 in relation to the transmitted signal, which yields the individual electromagnetic profile of the user. If comparison 6 of the reflected signal with the saved real-time profile 7 shows the coincidence, that is, no deviations was found, then the access signal 8 is continuously generated (fig. 1). As soon as secondary components mismatching with the previously defined profile appear in the received reflected signal (its spectrum), the signal of access termination is generated. A comparison 6 of the current individual electromagnetic profile with profiles from a profile library stored in the database 9 (fig. 2) is also possible. Based on results of such comparison, either access signal is generated or set of identification parameters 10 (a descriptor) is displayed.

Summary of the invention consists in the new method proposed by the authors for obtaining a stable, time-invariant profile of any biological object, including a human.

This substance can be realized as follows.

Embodiment 1 of the invention.

Embodiment 1 of the invention is presented by the dual channel probing as illustrated by a flow chart in figs. 1-3.

A probe signal is generated. To do this, signals of two frequencies f1, f2 in microwave and extremely high-frequency bands (from 1 to 300 GHz) are generated by at least two generators 11 (fig. 3). Then signals of generators 11 are modulated in width of radio-frequency pulses by modulators 12 using a white noise generator 13 (figs. 3, 4, 6). More particularly, signals of generators 11 are modulated by a pulse binary sequence with a random order of pulses (pulses correspond to "ones" and pauses to the "zeros") at clocked normalized pulse and pause duration (fig. 6). To achieve this, a white noise (digital (fig. 6) or analog) from the output of the generator 13 is passed through a digital filter 14 with a finite-duration impulse response and tunable coefficients and their output signal is supplied to modulators 12. So, modulated signals of generators 11 are pulse trains with random durations and random duration of pauses (fig. 5). These signals are further radiated by the antenna system 3 towards the biological object 1. Transmitted signals superpose inside tissues of the biological object and non-linearly transform. Spectrum of transmitted signal can be matched with the human body spectrum by means of tuning of transmitted signal carrier frequency produced by generators 11 (figs. 8-13). The signal that results from such transformation has a frequency matching with cellular and nuclear biomembranes. As a result, this signal becomes modulated by inherent acoustoelectric vibrations of biomembranes, which are stable for a given organism, but have good resolvable individual characteristics. The reflected signal that contains such components is received by remote antenna system 3 and fed to the receiver 4. The output signal of the receiver 4 is compared with the modulated signal at the output of digital filter 14, and the residual signal from the output of differential element 15, which is no else but error signal, is fed to the information input of neurocomputer 16. The neurocomputer comprising an adaptive hardware or virtual software neural network generates control signals arriving at the control inputs of the digital filter 14 and thereby sets the coefficient values of the filter 14. In such a way, a feedback is closed between probing and reflected signals due to the adaptive tuning of the modulating signal spectrum in respect to the reflected signal. The coefficient change dynamics for filter 14 is shown in fig. 7, where only one coefficient is presented as an example. It is seen that these dynamics is aimed to error minimization for modulated signal deviation from demodulated received signal at the output of receiver 4. The initial spectrum of summary signal produced by generators and transformed by non-linearities of the biological object, i.e. absorption signal, has a complex structure and is illustrated in fig. 14. Fig. 15 presents deviation of coefficients of the adaptive filter 14 from coefficients of the model of unknown system to be identified (biological object 1). The feedback action is apparent in adjusting coefficients of the adaptive filter 14 in such way that their values approach values of coefficients of model of the unknown system. Dynamics of this approach (law of time variation) is strictly individual for each organism, practically does not change over time during the mature age and can therefore serve as an identification descriptor used, inter alia, to get access to information or other systems. The authors of this invention have determined the optimal carrier signal frequency for generators 11 in order to reach the best matching between spectrum of summary signal produced by generators 11 and transformed by non-linearities of the biological object 1 tissues and spectrum of natural frequencies of the organism (figs. 8-13) and thereby facilitate the identification. It can be seen that in this case the reflected signal is the most informative one.

Embodiment 2 of the invention.

Embodiment 2 of the invention is presented by the multi-channel probing as illustrated by a flow chart in fig. 4. Embodiment 2 differs from the embodiment 1 in the following.

Several generators 11 simultaneously generate low-intensity (E < 1 μV/m) radio signals of different frequencies f1, f2, ..., fn in microwave and extremely high-frequency bands (from 1 to 300 GHz) to different radio channels. These signals are radiated by the antenna system 3 towards a biological object 1. Signals of each generator 11 are modulated in width of radio-frequency pulses by corresponding number of modulators 12. For this, the signal is passed through adaptive filters 4 connected with a white noise generator 13 (Figure 4), number of filters being equal to the number of channels and respectively number of generators 11. If some of frequencies f1, f2, ..., fn produced by generators 11 are multiples, then the number of adaptive filters may be less than the number of channels due to multiplexing channels with multiple frequencies per one filter

14.

Owing to increase in the number of probing signal channels, it is possible to extend the spectrum, which provides both more accurate and more informative superposition of spectra of absorbed summary signal and natural frequencies of biological object 1 (figs 8-13). This contributes to a more accurate identification of the individual electromagnetic profile.

EXAMPLE OF PARTICULAR EMBODIMENT

To prevent unauthorized access, a user was irradiated with a low-intensity (energy flux density P = 1 μW/m^2) microwave two-frequency signal simultaneously and concurrently via two channels according to embodiment 1 of the invention. Frequencies of the signals were equal to 17.0 and 34.02 GHz. These frequencies were chosen based on the best matching between mixed in the user's body signal spectrum and the user's body natural spectrum of acoustoelectric vibrations of nuclear and cellular biomembranes, reflecting combinations of geometry and electrodynamic parameters (bioelectrical activity, dielectric constant, etc.) of cellular structures unique for each user. The carrier frequency signals were modulated with a binary pulse sequence with a random (white noise) pulse repetition order (see fig. 6); the frequency of clock generator was equal to 5000 kHz. A reflected signal from the user was received by a separate antenna. After demodulation, the received signal was compared with a binary pulse sequence transmitted through a digital filter with a finite-duration impulse response and number of adjustable coefficients n=27. The error (mismatch) signal was applied to the inputs of an artificial neural network (neurocomputer), which automatically adjusted its weight coefficients and digital filter coefficients to minimize the error signal. In such manner, the feedback of reflected signal parameters (spectrum) with radiated signal parameters (spectrum) was closed. In course of such data processing, dynamics (time history) of digital filter coefficients change was recorded and stored until the system was balanced. If the user stopped irradiation and went off, the procedure was automatically resumed after the user return, and the new received characteristics of the digital filter coefficients dynamics were compared with the stored ones. If returned user was the same, characteristics remained the same too, and an access signal was generated. The system balancing time in this particular embodiment was 300 ms.

The proposed invention has the following advantages over known methods and authentication devices known to date from the state of the art:

- by applying new previously unknown operations and their order according to the proposed method, it becomes possible for the first time to determine the stable individual electromagnetic profile of any biological object including a human;
- by executing proposed actions under proposed conditions in proposed order, accuracy and reliability of authentication can be increased because the determined individual electromagnetic profile is time-invariant during life;
- since the proposed method has a high degree of unambiguous determination of individual information characteristics and a great protection against interference, accuracy of authentication can be increased due to exception of errors;
- due to impossibility to forge the identification parameters subject to determining according to the proposed method, access security during authentication is increased;
- due to full automation of the process excluding any special user actions, authentication procedure simplifies;
- since the proposed method does not require to keep in mind keys, passwords, or to carry any special devices (keys, cards, flash drives, mobile phones, etc.), operational capabilities become enhanced.

REFERENCE

1. Sharifov S.K., Stepanyan I.V., Savelyev A.V. Foundations of the innovative method of transcranial electromagnetic stimulation of the brain // Neurocomputers: development, application. 2017. # 5. P. 60-62.

2. Sharifov S.K. Research of the influence of radiation from Biomedis "Trinity" devices on intracellular processes // Biomedical radio electronics. 2018. # 10. in print.

CLAIMS

1. A method for automatic contactless authentication including remote irradiating a biological object with a probing radio signal, receipting the signal reflected from the biological object, fixation an individual unique time-stable electromagnetic profile of the object, and identification of the biological object based on this profile.
2. A method for automatic contactless authentication according to claim 1, wherein fixation an individual unique time-stable electromagnetic profile of biological object is carried out:

   a) generating a probing radio signal;

   whereby the probing signal is multifrequency and consists of at least two radio signals in the microwave and extremely high-frequency bands;

   whereby the radio signals in the microwave and extremely high-frequency bands are premodulated;

   b) radiating of the generated probing signal;

   c) information processing of the reflected signal.
3. A method for automatic contactless authentication according to claims 1 and 2, wherein the probing radio signal is modulated by a white noise signal.
4. A method for automatic contactless authentication according to claims 1 and 2, wherein the probing radio signal is modulated by a binary pulse sequence with a random order of codes corresponding to "zero" or "one".
5. A method for automatic contactless authentication according to claims 1 and 2, wherein a feedback is closed between the reflected signal and the probing signal;

   whereby the feedback between reflected and probing signals is closed by means of adaptive tuning of the modulating signal spectrum depending on the reflected signal.

6. A method for automatic contactless authentication according to claims 1 and 2, wherein irradiation of the biological object is low-intensity.
7. A method for automatic contactless authentication according to claims 1 and 2, wherein spectrum of biological object irradiation is matched with geometry and electrodynamic parameters (bioelectrical activity, dielectric constant, etc.) of biological object structures.
8. A method for automatic contactless authentication according to claims 1 and 2, wherein irradiation frequency range is matched with the frequency of acoustoelectric vibrations of the nuclear membranes.
9. A method for automatic contactless authentication according to claims 1 and 2, wherein irradiation frequency range is matched with the frequency of acoustoelectric vibrations of cell membranes.
10. A method for automatic contactless authentication according to claims 1 and 2, wherein frequency of generated probing radio signal lies within the range of 1-300 GHz.
11. A method for automatic contactless authentication according to claims 1 and 2, wherein tissues of biological object subjected to irradiation with radio signals in the microwave and extremely high-frequency bands are used as a broadband nonlinear mixer.
12. A method for automatic contactless authentication according to claim 2, wherein the information processing is carried out:

    a) using an adaptive artificial neural network;

    b) using a virtual neural network.
13. A method for automatic contactless authentication according to claim 12, wherein the information processing of the signal includes fixation of the dynamics of adaptation parameters of the biotechnical system consisting of organism of

biological object and a probing device.

14. A method for automatic contactless authentication according to claim 13, wherein the information processing of the signal includes time-history analysis of adaptation parameters of the biotechnical system consisting of organism of biological object and a probing device.

15. A method for automatic contactless authentication according to claims 1, 2, and 14, wherein time-history of adaptation parameters is compared with a reference and an access signal is continuously generated based on results of the comparison.

16. A method for automatic contactless authentication according to claims 1, 2, and 14, wherein time-history of adaptation parameters is compared with a database in the single-pulse mode and, when matching, the identification parameters are displayed.

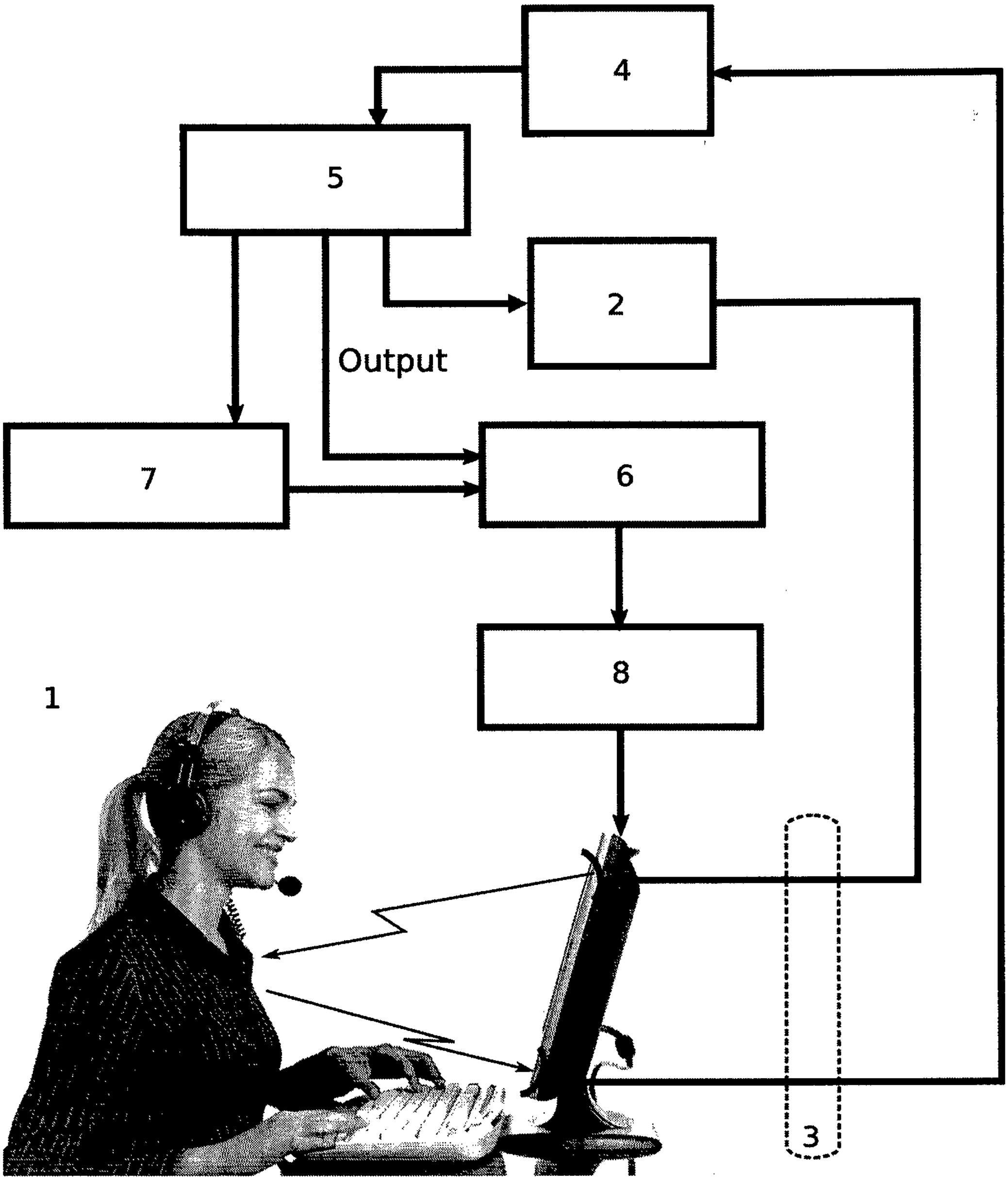

Fig. 1

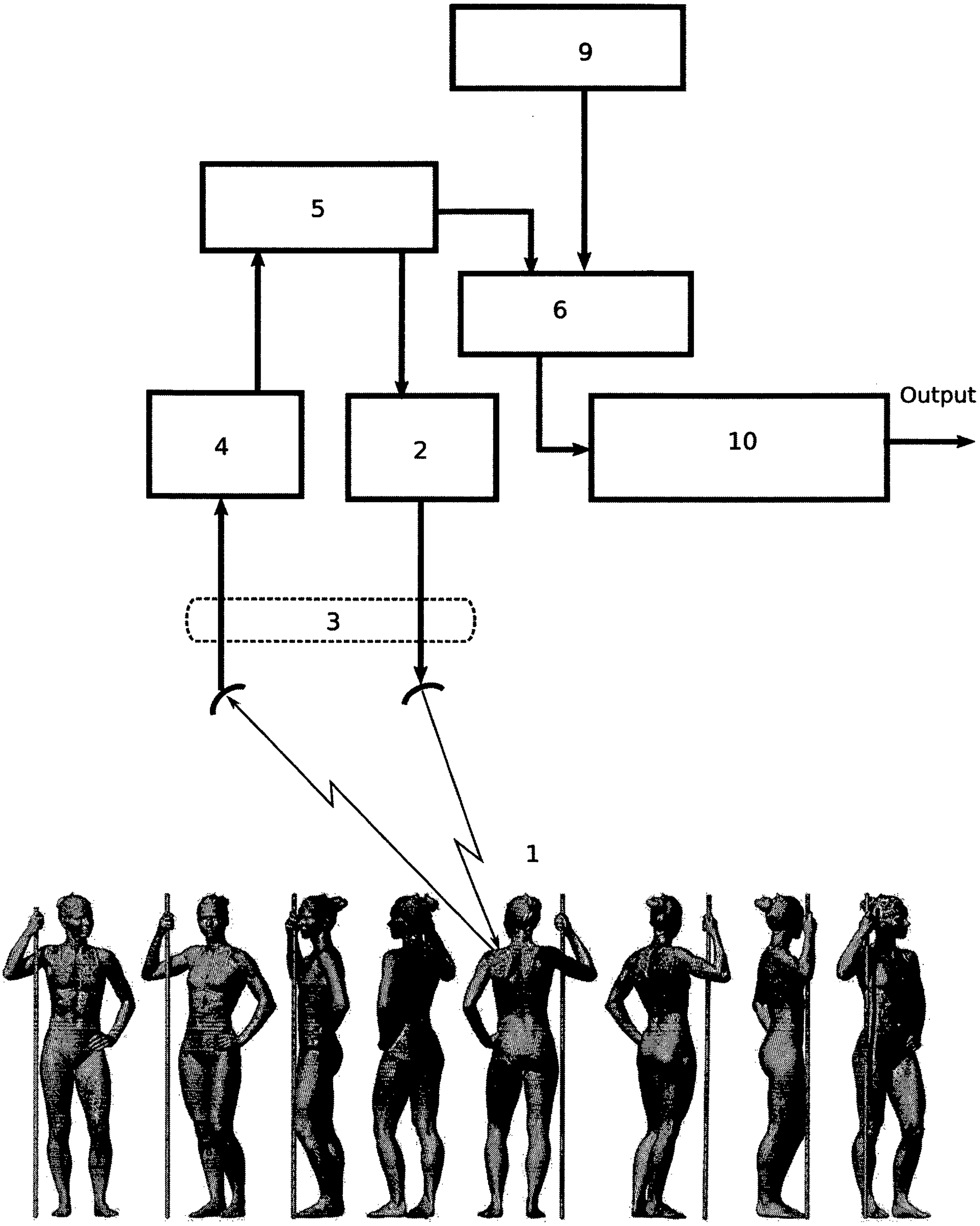

Fig. 2

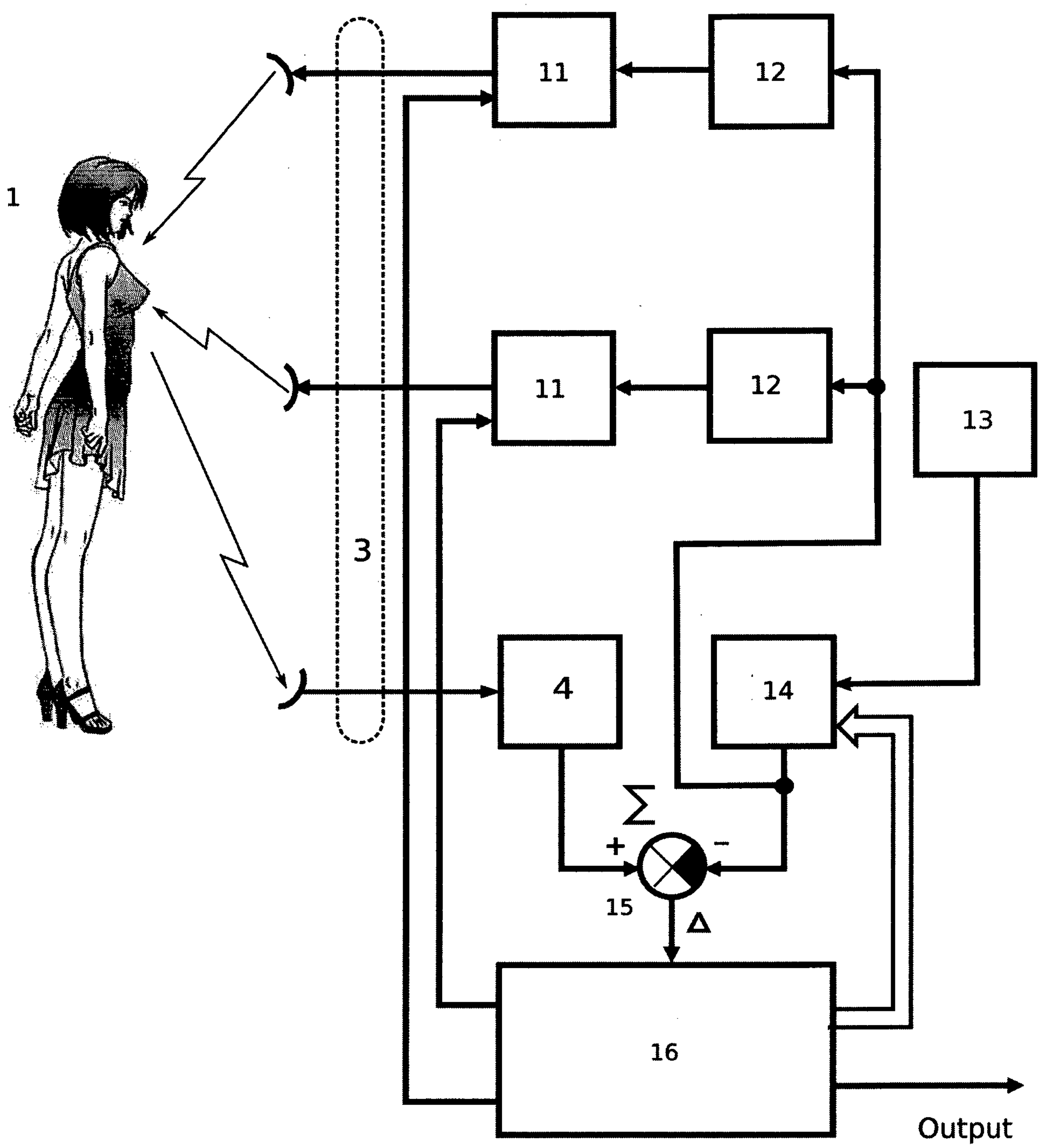

Fig. 3

METHOD OF NON-CONTACT AUTOMATIC AUTHENTICATION

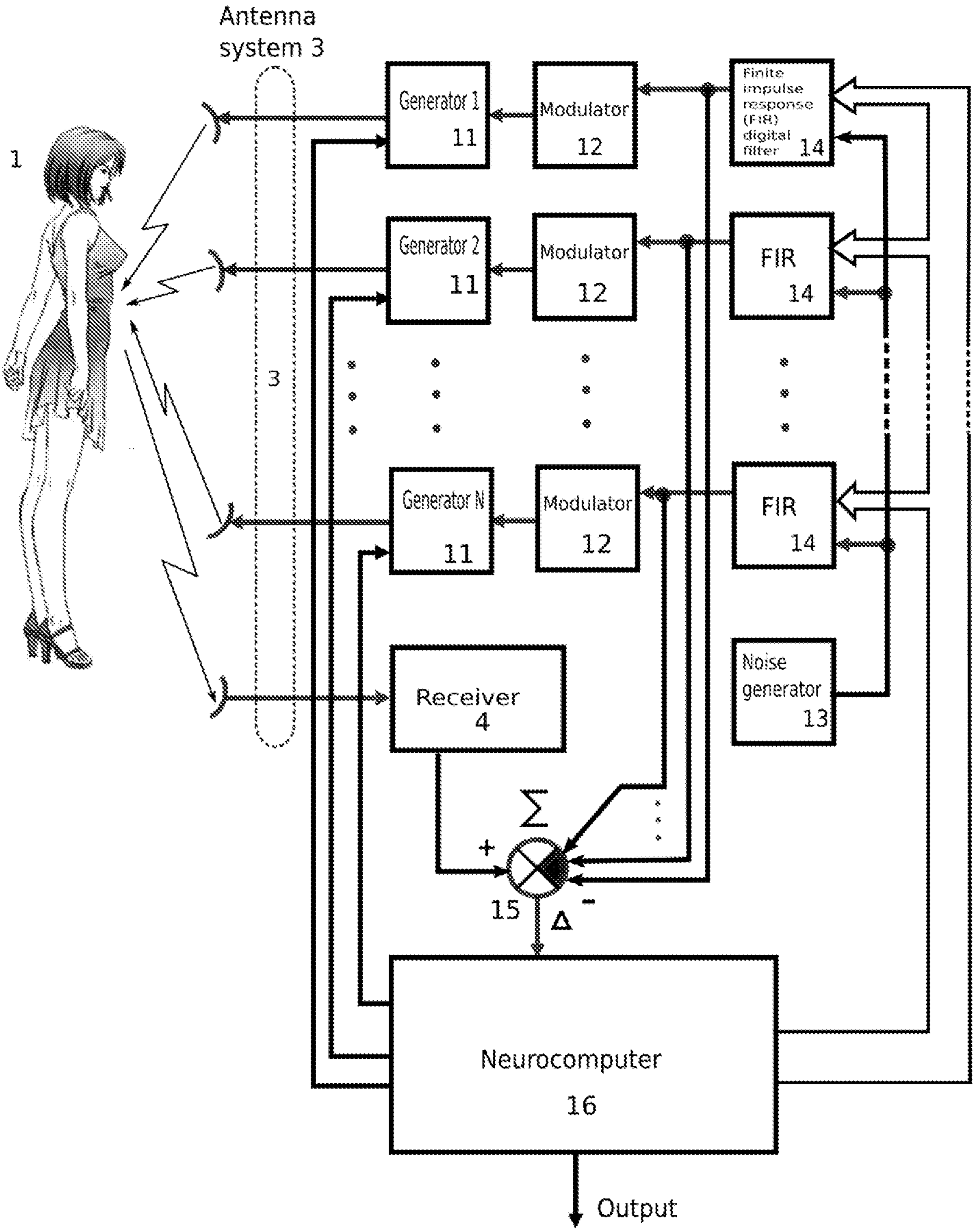

Fig. 4

Author: S.K-ogly Sarifov

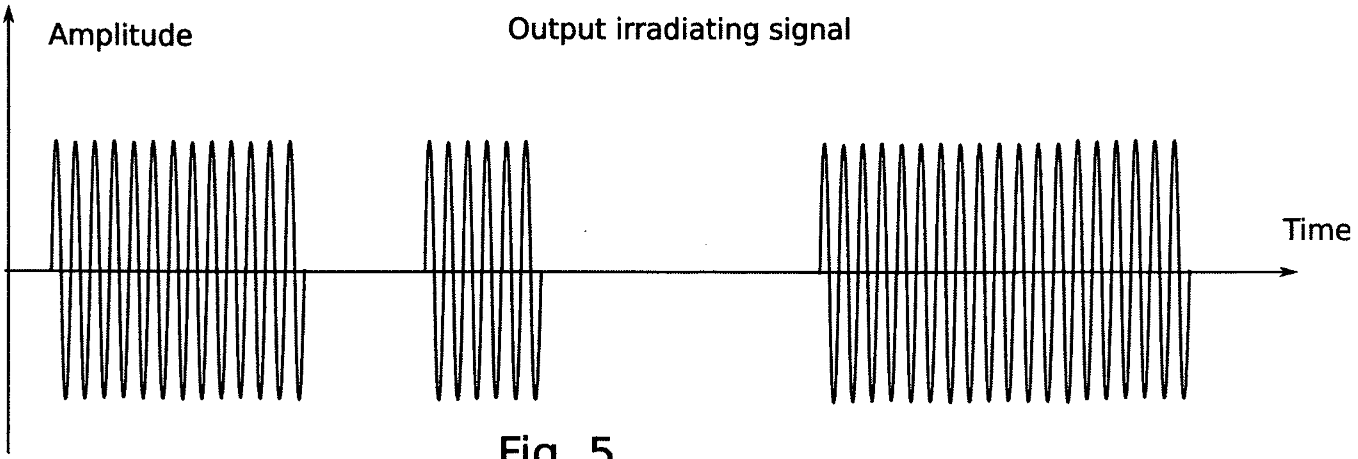

Fig. 5

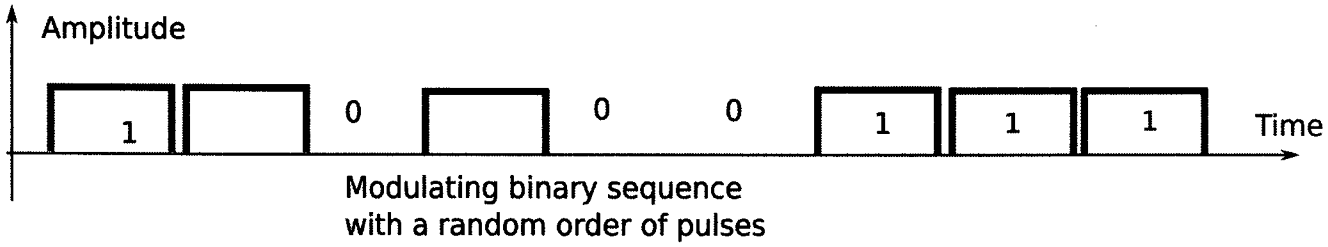

Fig. 6

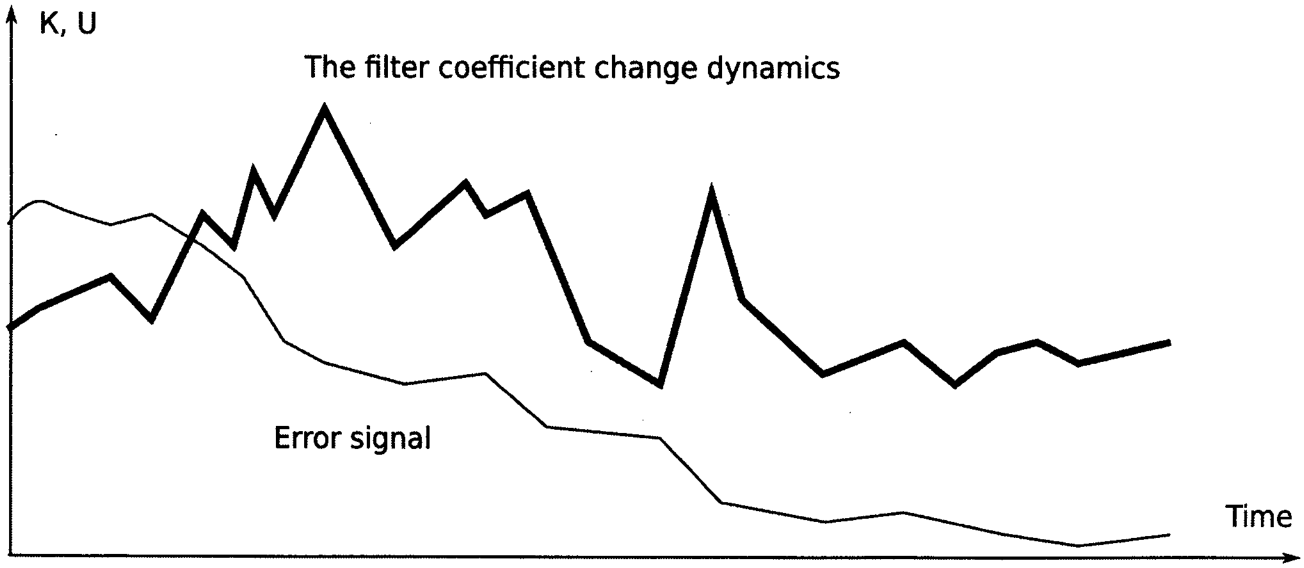

Fig. 7

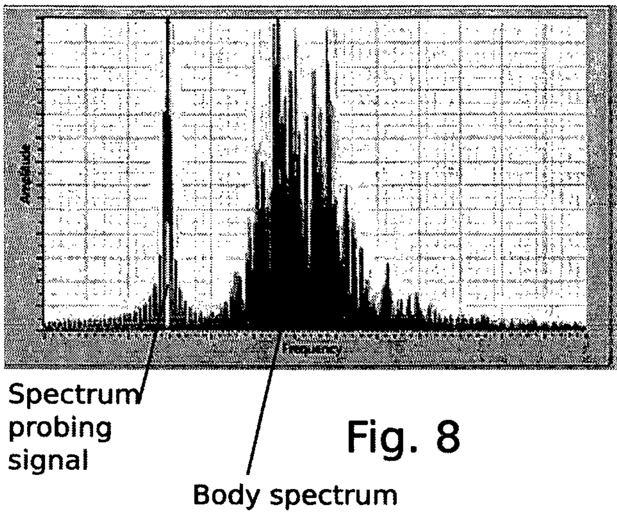

Fig. 8

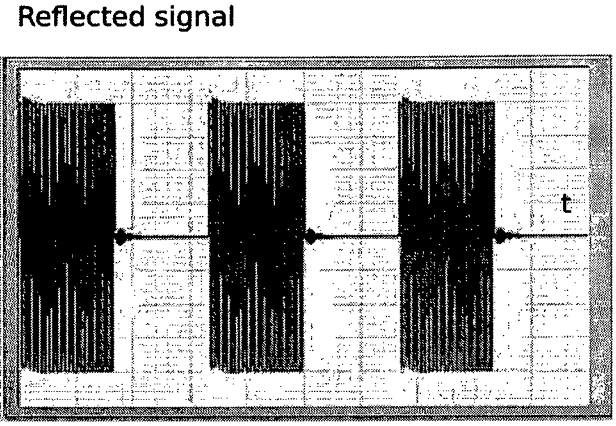

Fig. 9

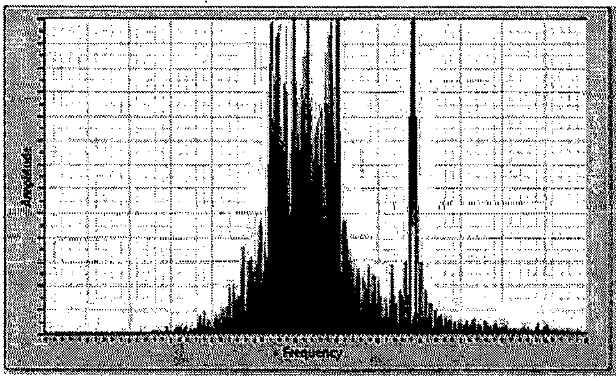

Fig. 10

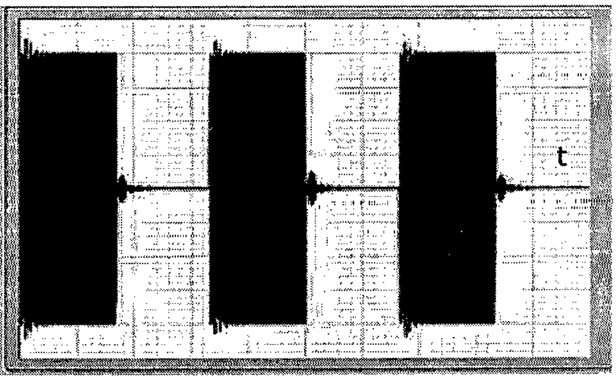

Fig. 11

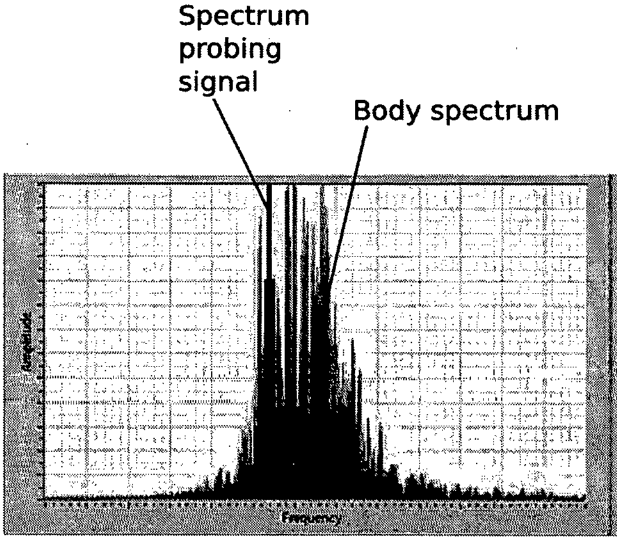

Fig. 12

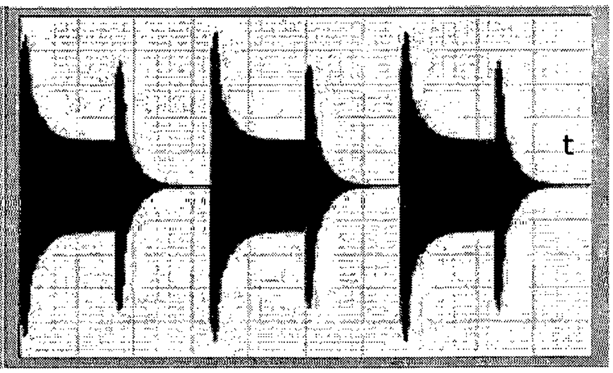

Fig. 13

Spectrum of the mixed probing signal

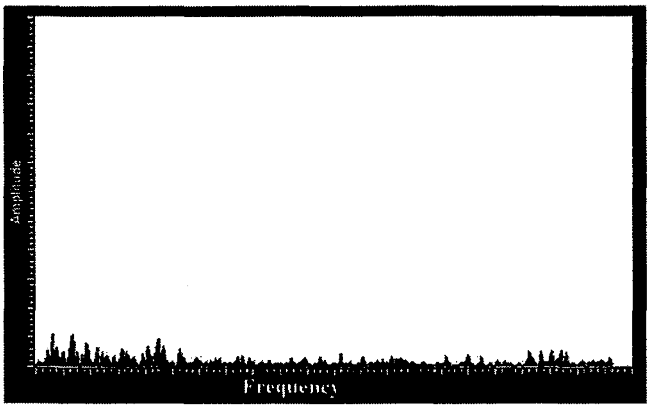

Fig. 14

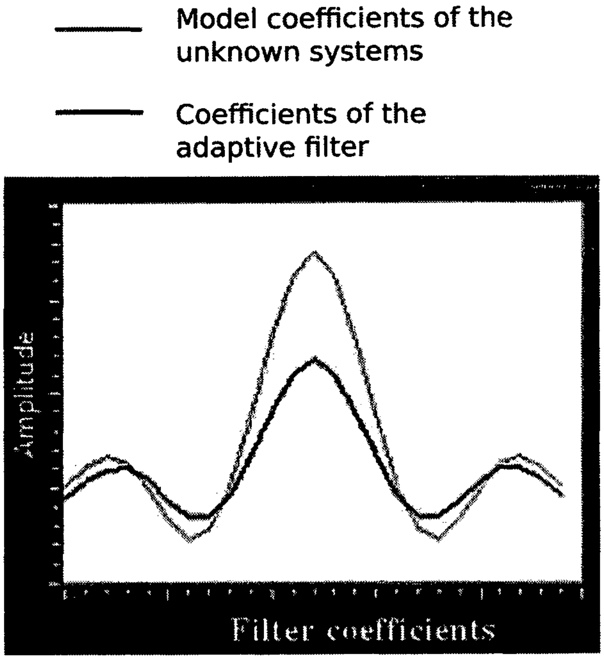

Fig. 15

The change in the spectrum of the mixed probing signal
when adjusting the filter coefficients

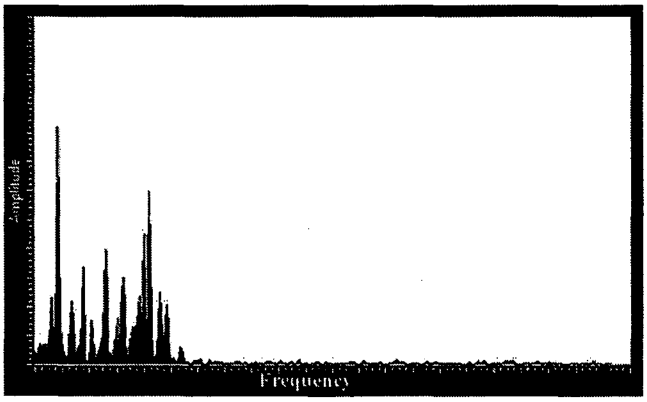

Fig. 16

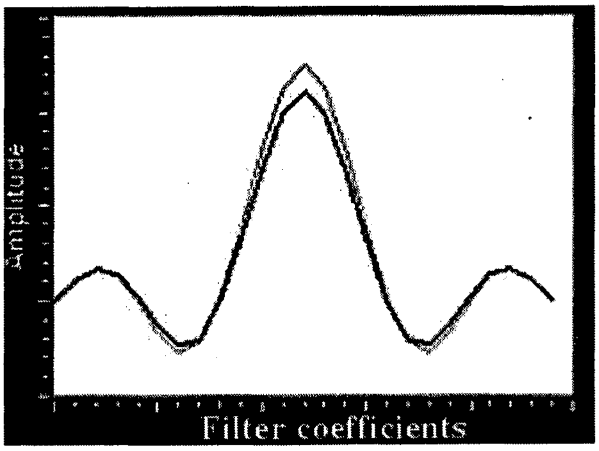

Fig. 17

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2018/001074

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06K9/00

ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FENG LIN ET AL: "Cardiac Scan : A Non-contact and Continuous Heart-based User Authentication System", PROCEEDINGS OF THE 23RD ANNUAL INTERNATIONAL CONFERENCE ON MOBILE COMPUTING AND NETWORKING , MOBICOM '17, 1 January 2017 (2017-01-01), pages 315-328, XP055590069, New York, New York, USA DOI: 10.1145/3117811.3117839 ISBN: 978-1-4503-4916-1 sections 1-7, 9 abstract; figures 1-16 ----- -/--	1-16

☒ Further documents are listed in the continuation of Box C.

□ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

21 May 2019

Date of mailing of the international search report

29/05/2019

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Nilsson, Martin

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2018/001074

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DIEDERICHS KAILTYN ET AL: "Wireless Biometric Individual Identification Utilizing Millimeter Waves", IEEE SENSORS LETTERS, IEEE, vol. 1, no. 1, 1 February 2017 (2017-02-01), pages 1-4, XP011642852, DOI: 10.1109/LSENS.2017.2673551 [retrieved on 2017-03-15] sections I-V; abstract; figures 1-6 -----	1-16