FORM 2

THE PATENTS ACT, 1970

(39 of 1970)

&

The Patent Rules, 2003

COMPLETE SPECIFICATION

(See section 10 and rule 13)

TITLE OF THE INVENTION

“A SYSTEM FOR FINGERPRINT IMAGE PROCESSING FOR AN ELECTRONIC DEVICE AND METHOD THEREOF”

We, applicant(s)

NAME	NATIONALITY	ADDRESS
1. Dr.S.Mani Naidu	INDIAN	Professor of Physics, Department of Physics, Vel Tech, Rangarajan Dr. Sagunthala R & D Institute of Science and Technology (Deemed to be University), Avadi, Chennai, Tamil Nadu, India. Pin Code:600062
2. Mrs.Ketha Santhi	INDIAN	Educational Consultant, Animation Department, College of Fine Arts, YSR Architecture and Fine Arts University, YSR Kadapa, Andhra Pradesh, India. Pin Code: 516162
3. Mrs.Jangam J.S.Mani	INDIAN	Assistant Professor, Department of Computer Applications, O/o Commissionerate of Collegiate Education-AP, Vijayawada, Andhra Pradesh, India. Pin Code: 521108
4. Dr.Armstrong Joseph	INDIAN	Professor, Sri Venkateswara College of Engineering & Technology (Autonomous), Chittoor, Andhra Pradesh, India. Pin Code:517127

5. Dr.C.S.Boopathi	INDIAN	Associate Professor, Department of EEE, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India. Pin Code:603203
6. Mr.Jadapalli Sreedhar	INDIAN	Assistant Professor, Department of EEE, Vignana Bharathi Institute of Technology, Aushapur (village), Hyderabad. Telangana, India. Pin Code:501301
7. Dr.Sushma Jaiswal	INDIAN	Assistant Professor, Department of Computer Science & Information Technology (CSIT), Guru Ghasidas Vishwavidyalaya (A Central University), Koni, Bilaspur, Chhattisgarh, India. Pin Code: 495009
8. Dr.Vemula Ramadevi	INDIAN	Assistant Professor, Department of ECE, CVR College of Engineering, Ibrahimpatnam, Hyderabad, Telangana, India. Pin Code:501510
9. Ms.G.Priyadharsini	INDIAN	Assistant Professor, Department of Mathematics, Kongu Arts And Science College, Erode, Tamil Nadu, India. Pin Code:638107
10. Mr.Tarun Jaiswal	INDIAN	Research Scholar, Department of Computer Application, National Institute of Technology (NITRR), Raipur, Chhattisgarh, India. Pin Code:492010

The following specification particularly describes the nature of the invention and the manner in which it is performed:

FIELD OF THE INVENTION

[001] The present invention relates to the field of the fingerprint image processing method for smartphone or any electronic device by using machine learning interfaces. The invention more particularly relates to a machine learning based system for user identification and authorized access to the electronic device through fingerprint verification and method thereof.

BACKGROUND OF THE INVENTION

[002] The following description provides the information that may be useful in understanding the present invention. It is not an admission that any of the information provided herein is prior art or relevant to the presently claimed invention, or that any publication specifically or implicitly referenced is prior art.

[003] Fingerprint recognition generally performs by way of collecting the texture of the surface of the hand fingerprint of the user through an array to obtain a fingerprint image. At present, common fingerprint recognition technologies include, but not limited to, capacitive, photoelectric, and ultrasonic.

[004] When the user places a finger on the touch screen of the electronic device, the skin and the conductor plate of the touch screen constitute a capacitance for further receiving the input. Since the distance between the ridges and valleys of fingerprints at different points is not equal, the capacitance of each unit varies with the distance between the fingerprint ridges and the valleys. Because of this different voltages are generated according to the capacitance of each unit, and eventually, fingerprints can be obtained and moved for image processing and verification through embedded software provided with the electronic device.

[005] Various Artificial intelligence and machine learning methods are known in computer science and are used to image processing and verification through embedded software provided with these electronic devices. However, a need exists for techniques that widen the range of potentially enhanced the securities for accessing the electronic device and that leverage machine learning techniques to produce more accurate predictions by using limited hardware interface and power usage.

[006] Considering the above drawbacks, accordingly, there remains a need in the prior art for a technical convergence to make an intelligent fingerprint image processing system, interfaces, using machine learning method, it is in this context that the present invention provides a machine learning based system for user identification and authorized access to the electronic device through fingerprint verification and method thereof, which provides herein a platform for fingerprint security and user device access authentication based on extraction of stored data with less efforts by user and limited hardware and power consumption of the device. Therefore, it would be useful and desirable to have a system and interface to meet the above-mentioned needs.

SUMMARY OF THE PRESENT INVENTION

[007] In view of the foregoing disadvantages inherent in the known types of conventional fingerprint verification system, method and devices for electronic devices, are now present in the prior art, the present invention provides a a machine learning based system for user identification and authorized access to the electronic device through fingerprint verification and method thereof.

The system is designed with, but not limited to, at least two set equipment implementation phase, in which the first set of equipment is the capturing fingerprint data through the hardware unit and these data are further passed on to the processing unit using matching and monitoring module, which is communicatively coupled with the second set of equipment implemented with the help of a machine learning interface for processing the data and generates the final authentication on the electronic device to the user, which has all the advantages of the prior art and none of the disadvantages.

[008] The main aspect of the present invention is to provide a system, which comprises an apparatus for fingerprint identification method and terminal, that can carry while ensuring fingerprint authentication safety with efficiency of highly secure fingerprint authentication by using artificial intelligence and machine learning.

[009] Another aspect of the present invention is to provide a system, in which first the system obtains a fingerprint image of the user and also detect finger touches humidity value during fingerprint recognition interface. If described humidity value is in default moistness value range, extract the characteristic of described fingerprint image by the processing unit so that it to be carried out Match cognization.

[010] The proposed system and method is implemented on, but not limited to, the Field Programmable Gate Arrays (FPGAs) and the like, PC, Microcontroller and with other known processors to have computer algorithms and instruction up gradation for supporting many applications domain where the aforesaid problems to solution is required.

[011] In this respect, before explaining at least one object of the invention in detail, it is to be understood that the invention is not limited in its application to the details of set of rules and to the arrangements of the various models set forth in the following description or illustrated in the drawings. The invention is capable of other objects and of being practiced and carried out in various ways, according to the need of that industry. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting.

[012] These together with other objects of the invention, along with the various features of novelty which characterize the invention, are pointed out with particularity in the disclosure. For a better understanding of the invention, its operating advantages and the specific objects attained by its uses, reference should be made to the accompanying drawings and descriptive matter in which there are illustrated preferred embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[013] The invention will be better understood and objects other than those set forth above will become apparent when consideration is given to the following detailed description thereof. Such description makes reference to the annexed drawings wherein:

[014] FIG. 1 illustrates a schematic diagram of a fingerprint image processing method for smartphone or any electronic device, in accordance with an embodiment of the present invention; and

[015] FIG. 2 illustrates a block diagram of the fingerprint image processing method for smartphone or any electronic device, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[016] While the present invention is described herein by way of example using embodiments and illustrative drawings, those skilled in the art will recognize that the invention is not limited to the embodiments of drawing or drawings described and are not intended to represent the scale of the various components. Further, some components that may form a part of the invention may not be illustrated in certain figures, for ease of illustration, and such omissions do not limit the embodiments outlined in any way. It should be understood that the drawings and detailed description thereto are not intended to limit the invention to the particular form disclosed, but on the contrary, the invention is to cover all modifications, equivalents, and alternatives falling within the scope of the present invention as defined by the appended claims. As used throughout this description, the word "may" is used in a permissive sense (i.e. meaning having the potential to), rather than the mandatory sense, (i.e. meaning must). Further, the words "a" or "an" mean "at least one” and the word “plurality” means “one or more” unless otherwise mentioned. Furthermore, the terminology and phraseology used herein is solely used for descriptive purposes and should not be construed as limiting in scope. Language such as "including," "comprising," "having," "containing," or "involving," and variations thereof, is intended to be broad and encompass the subject matter listed thereafter, equivalents, and additional subject matter not recited, and is not intended to exclude other additives, components, integers or steps. Likewise, the term "comprising" is considered synonymous with the terms "including" or "containing" for applicable legal purposes. Any discussion of documents, acts, materials, devices, articles and the like is included in the specification solely for the purpose of providing a context for the present invention. It is not suggested or represented that any or all of these matters form part of the prior art base or were common general knowledge in the field relevant to the present invention.

[017] In this disclosure, whenever a composition or an element or a group of elements is preceded with the transitional phrase “comprising”, it is understood that we also contemplate the same composition, element or group of elements with transitional phrases “consisting of”, “consisting”, “selected from the group of consisting of, “including”, or “is” preceding the recitation of the composition, element or group of elements and vice versa.

[018] The present invention is described hereinafter by various embodiments with reference to the accompanying drawings, wherein reference numerals used in the accompanying drawing correspond to the like elements throughout the description. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiment set forth herein. Rather, the embodiment is provided so that this disclosure will be thorough and complete and will fully convey the scope of the invention to those skilled in the art. In the following detailed description, numeric values and ranges are provided for various aspects of the implementations described. These values and ranges are to be treated as examples only and are not intended to limit the scope of the claims. In addition, a number of materials are identified as suitable for various facets of the implementations. These materials are to be treated as exemplary and are not intended to limit the scope of the invention.

[019] Referring now to the drawings, these are illustrated in **FIG. 1-2**, the present invention discloses a system for fingerprint image processing for an electronic device and method thereof. The system is comprised of, but not limited to, a monitoring unit provided to monitor an operation performed on a scanning area of the electronic device; and a sending unit configured to send a wake-up call to a fingerprint scanning unit when the operation indicating the entry into a pre-set fingerprint application scenario is detected, where the wake-up call is used to instruct the fingerprint scanning unit to enter the working mode.

[020] In accordance with another embodiment of the present invention, the processing unit is configured to analyse whether a fingerprint image meets an authorization condition corresponding to the pre-set fingerprint application scenario detection, where the pre-stored fingerprint image is based on the preset fingerprint application scenario, the resolution is stored.

[021] In accordance with another embodiment of the present invention, the sending unit is further configured to send a sleep instruction to the fingerprint scanning unit when receiving an operation indicating to enter a fingerprint application scenario other than the pre-set fingerprint application scenario by the entering user.

[022] In accordance with another embodiment of the present invention, the system is further comprised of, but not limited to, a slowly varying and a low-frequency skin image and spatially filtering the skin image to remove low-frequency spatial image compliments using a real-time full-frame rate system.

[023] In accordance with another embodiment of the present invention, the sending unit is having a fingerprint determination unit for determining a dryness level of the finger and a current fingerprint image of the finger of the user, and configured to determine a fingerprint image enhancement parameter corresponding to the dryness level.

[024] In accordance with another embodiment of the present invention, the processing unit is having a fingerprint matching unit configured for matching the processed fingerprint image with a preset fingerprint application scenario after the processing unit prforms optimization processing on the fingerprint image according to the image enhancement parameters so as to be used for user fingerprint identification.

[025] In accordance with another embodiment of the present invention, the fingerprint image enhancement parameter includes, but not limited to, image contrast, image resolution, and image color and the processing unit is configured to provide optimization processing on the fingerprint image according to the image enhancement parameters.

[026] In accordance with another embodiment of the present invention, the scanning area of the fingerprint scanning unit is provided larger than the scanning area of the preset fingerprint application fingerprint scanning unit, and the resolution of the preset fingerprint application fingerprint scanning unit is greater than the resolution of the fingerprint scanning module.

[027] Further, various exemplary computer system for implementing embodiments consistent with the present disclosure. Variations of computer system may be used for implementing the system for fingerprint image processing for an electronic device. Computer system may comprise a central processing unit ("CPU" or "processor"). Processor may comprise at least one data processor for executing program components for executing user or system-generated requests. A user may include a person, a person using a device such as such as those included in this disclosure, or such a device itself. The processor may include specialized processing units such as integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc. The processor may include a microprocessor, such as AMD Athlon, Duron or Opteron, ARM’s application, embedded or secure processors, IBM PowerPC, Intel’s Core, Itanium, Xeon, Celeron or other line of processors, etc. The processor may be implemented using mainframe, distributed processor, multi-core, parallel, grid, or other architectures. Some embodiments may utilize embedded technologies like application-specific integrated circuits (ASICs), digital signal processors (DSPs), Field Programmable Gate Arrays (FPGAs), etc.

[028] Processor may be disposed in communication with one or more input/output (I/O) devices via I/O interfaces. The I/O interfaces may employ communication protocols/methods such as, without limitation, audio, analog, digital, monoaural, RCA, stereo, IEEE-1394, serial bus, universal serial bus (USB), infrared, PS/2, BNC, coaxial, component, composite, digital visual interface (DVI), high-definition multimedia interface (HDMI), RF antennas, S-Video, VGA, IEEE 802.n /b/g/n/x, Bluetooth, cellular (e.g., code-division multiple access (CDMA), high-speed packet access (HSPA+), global system for mobile communications (GSM), long-term evolution (LTE), WiMax, or the like), etc.

[029] In some embodiments, the processor may be disposed in communication with one or more memory devices (e.g., RAM, ROM, etc.) via a storage interface. The storage interface may connect to memory devices including, without limitation, memory drives, removable disc drives, etc., employing connection protocols such as serial advanced technology attachment (SATA), integrated drive electronics (IDE), IEEE-1394, universal serial bus (USB), fiber channel, small computer systems interface (SCSI), etc. The memory drives may further include a drum, magnetic disc drive, magneto-optical drive, optical drive, redundant array of independent discs (RAID), solid-state memory devices, solid-state drives, etc. The memory devices may store a collection of program or database components, including, without limitation, an operating system, user interface application, web browser, mail server, mail client, user/application data (e.g., any data variables or data records discussed in this disclosure), etc. The operating system may facilitate resource management and operation of the computer system. Examples of operating systems include, without limitation, Apple Macintosh OS X, Unix, Unix-like system distributions (e.g., Berkeley Software Distribution (BSD), FreeBSD, NetBSD, OpenBSD, etc.), Linux distributions (e.g., Red Hat, Ubuntu, Kubuntu, etc.), IBM OS/2, Microsoft Windows (XP, Vista/7/8, etc.), Apple iOS, Google Android, Blackberry OS, or the like.

[030] The word “module,” “model” “algorithms” and the like as used herein, refers to logic embodied in hardware or firmware, or to a collection of software instructions, written in a programming language, such as, for example, Java, C, Python or assembly. One or more software instructions in the modules may be embedded in firmware, such as an EPROM. It will be appreciated that modules may comprised connected logic units, such as gates and flip-flops, and may comprise programmable units, such as programmable gate arrays or processors. The modules described herein may be implemented as either software and/or hardware modules and may be stored in any type of computer-readable medium or other computer storage device. Further, in various embodiments, the processor is one of, but not limited to, a general-purpose processor, an application specific integrated circuit (ASIC) and a field-programmable gate array (FPGA) processor. Furthermore, the data repository may be a cloud-based storage or a hard disk drive (HDD), Solid state drive (SSD), flash drive, ROM or any other data storage means.

[031] The above-mentioned system is having various novel aspects such as, but not limited to, the processing unit with the machine learning interface for providing a machine learning based system user fingerprint identification and method thereof, by the present invention and which will be understood by reading and studying the aforesaid embodiments, and further, the system is described which can also be implemented the aforesaid steps of the fingerprint image processing method according to any below mentioned claims with at most slight modification with the same advantages described above.

[032] It is to be understood that the above description is intended to be illustrative, and not restrictive. For example, the above-discussed embodiments may be used in combination with each other. Many other embodiments will be apparent to those of skill in the art upon reviewing the above description.

[033] The benefits and advantages which may be provided by the present invention have been described above with regard to specific embodiments. These benefits and advantages, and any elements or limitations that may cause them to occur or to become more pronounced are not to be construed as critical, required, or essential features of any or all of the embodiments.

[034] While the present invention has been described with reference to particular embodiments, it should be understood that the embodiments are illustrative and that the scope of the invention is not limited to these embodiments. Many variations, modifications, additions and improvements to the embodiments described above are possible. It is contemplated that these variations, modifications, additions and improvements fall within the scope of the invention.

We Claim:

1. A system for fingerprint image processing for an electronic device, comprising:

a monitoring unit provided to monitor an operation performed on a scanning area of the electronic device; and

a sending unit configured to send a wake-up call to a fingerprint scanning unit when the operation indicating the entry into a preset fingerprint application scenario is detected, where the wake-up call is used to instruct the fingerprint scanning unit to enter the working mode.

2. The system as claimed in claim **1**, wherein a processing unit is configured to analyse whether a fingerprint image meets an authorization condition corresponding to the preset fingerprint application scenario detection, where the pre-stored fingerprint image is based on the preset fingerprint application scenario, the resolution is stored.

3. The system as claimed in claim **1**, wherein the sending unit is further configured to send a sleep instruction to the fingerprint scanning unit when receiving an operation indicating to enter a fingerprint application scenario other than the preset fingerprint application scenario by the entering user.

4. The system as claimed in claim **1**, wherein the sending unit is having a fingerprint determination unit for determining a dryness level of the finger and a current fingerprint image of the finger of the user, and configured to determine a fingerprint image enhancement parameter corresponding to the dryness level.

5. The system as claimed in claim **1**, wherein the processing unit is having a fingerprint matching unit configured for matching the processed fingerprint image with a preset fingerprint application scenario after the processing unit performs optimization processing on the fingerprint image according to the image enhancement parameters so as to be used for user fingerprint identification.

6. The system as claimed in claim **1**, wherein the fingerprint image enhancement parameter includes, but not limited to, image contrast, image resolution, and image color and the processing unit is configured to provide optimization processing on the fingerprint image according to the image enhancement parameters.

7. The system as claimed in claim **1**, wherein the scanning area of the fingerprint scanning unit is provided larger than the scanning area of the preset fingerprint application fingerprint scanning unit, and the resolution of the preset fingerprint application fingerprint scanning unit is greater than the resolution of the fingerprint scanning module.

8. The system as claimed in claim **1**, wherein a memory unit and a computer program stored on the memory unit and executable on the processing unit, the computer program, when executed by the processing unit, implementing the steps of the fingerprint image processing method according to any one of claims 1 to 7.

Dated this 30th day of November 2021

Signature: Smaninaidu

Applicant(s)

Dr.S.Mani Naidu et. al.

ABSTRACT

A SYSTEM FOR FINGERPRINT IMAGE PROCESSING FOR AN
ELECTRONIC DEVICE AND METHOD THEREOF

[035] The present invention discloses a system for fingerprint image processing for an electronic device and method thereof. The system includes, but not limited to, a monitoring unit provided to monitor an operation performed on a scanning area of the electronic device; and a sending unit configured to send a wake-up call to a fingerprint scanning unit when the operation indicating the entry into a pre-set fingerprint application scenario is detected, where the wake-up call is used to instruct the fingerprint scanning unit to enter the working mode.

Accompanied Drawing **[FIG. 1]**

Dated this 30th day of November 2021

Signature: Smaninaidu

Applicant(s)

Dr.S.Mani Naidu et. al.