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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 August 2013 (08.08.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/116117 A1

(51) International Patent Classification:
G06F 21/32 (2013.01)

(21) International Application Number:
PCT/US2013/023302

(22) International Filing Date:
25 January 2013 (25.01.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/362, 896 31 January 2012 (31.01.2012) US

(71) Applicant: **Google Inc.** [US/US]; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US).

(72) Inventors: **WUELLNER, Trond**; 157 Easy Street, Mountain View, CA 94043 (US). **CAIRNS, Ryan**; 1570 Wakefield Terrace, Los Altos, CA 94024 (US).

(74) Agent: **ITRI, Mark J.**; McDermott Will & Emery LLP, 4 Park Plaza, Suite 1700, Irvine, CA 92614 (US).

(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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, 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, ML, MR, NE, SN, TD, TG).

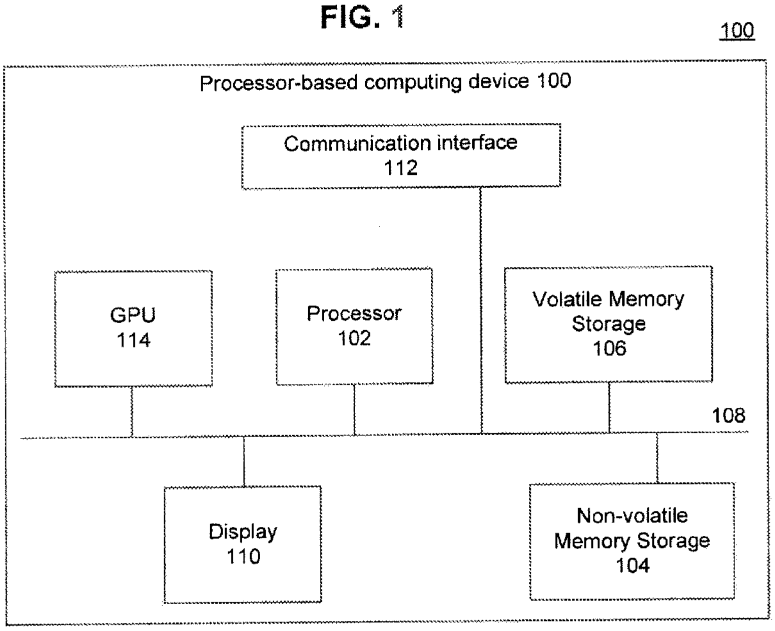
Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: FACIAL RECOGNITION STREAMLINED LOGIN

FIG. 1


100
Processor-based computing device 100
Communication interface 112
GPU 114
Processor 102
Volatile Memory Storage 106
108
Display 110
Non-volatile Memory Storage 104

(57) **Abstract**: A system and method are disclosed for providing login credentials to a computer system using a biometric indicator. The system includes an image comparison module, a user interface, and an access control module. The image comparison module is configured to compare an image of a user, requesting login access to a client device, with images in a database to determine whether the image matches an image in the database. The user interface is configured to receive input from the image comparison module and to prompt the user for login credentials based on the input received from the comparison module. The access control module is configured to grant or deny login access to the user based on the user input that is entered in response to the prompting.

FACIAL RECOGNITION STREAMLINED LOGIN

Inventors: Trond Wuellner
Ryan Cairns

BACKGROUND

Field

[0001] This disclosure relates to systems and methods for providing login credentials for computer systems.

Background Art

[0002] Passwords are used in many ways to protect data systems and networks. For example, passwords are used to authenticate users of operating systems, applications such as email, remote access, etc. Passwords are also used to protect files and other stored information such as, for example, compressed files, cryptographic keys, or encrypted hard drives. Online transactions such as shopping, banking, communications, and file exchange have become commonplace. Online transactions, however, are susceptible to attack by unscrupulous entities that may intercept passwords or otherwise gain access to login credentials. Identity theft is a consequence of Internet commerce that, unfortunately, is also becoming commonplace. When passwords or identities are stolen, the security of email, online file repositories, bank accounts, etc., may be compromised.

[0003] In order to retain high security, it is important for users to use passwords that are sufficiently complex so that they cannot be easily broken and to use a different password for each application requiring a password.

[0004] For added security, some applications require multi-factor authentication. Authentication can require several factors such as a password, use of a smart card, or a biometric indicator (e.g., voice recognition, fingerprint, retinal scan, etc.). Single-factor authentication may rely on one of the three forms of authentications, such as a password, while two- or three-factor authentications may use two or three factors, respectively. Although the use of multi-factor authentication increases the difficulty for a third party to gain access to a system, password-based, single-factor authentication is still currently the most commonly used authentication method.

BRIEF SUMMARY

[0005] Systems and methods are disclosed for providing login credentials to a computer system using a biometric indicator for added security and convenience.

[0006] In an embodiment, a system is disclosed for providing login credentials to a computer-based system. Such a system is implemented on a processor-based computing device. The system includes an image comparison module, a user interface, and an access control module. The image comparison module is configured to compare an image of a user requesting login access to a client device with images in a database, to determine whether the image matches an image in the database. The user interface is configured to receive input from the image comparison module and to prompt the user for login credentials based on the input received from the comparison module. The input can take the form of a reduced set of login credentials or a complete set of login credentials depending on whether or not a correct match is found. The access control module is configured to grant or deny login access to the user based on the user input that is entered in response to the prompting. The user interface is further configured to prompt the user to enter one of the following based on the result of the comparison: (1) a reduced set of login credentials when a correct match is found, or (2) a complete set of login credentials when no match is found or when an incorrect match is found.

[0007] The access control module is further configured to: (1) grant login access to the user when a complete set of login credentials is entered that correspond to an authorized user, (2) grant login access to the user when a reduced set of login credentials is entered that correspond to an authorized user whose image was matched by an image in the database, or (3) deny user login access otherwise.

[0008] Further features and advantages as well as the structure and operation of various embodiments are described in detail below with reference to the accompanying drawings. It is noted that the invention is not limited to the specific embodiments described herein. Such embodiments are presented herein for illustrative purposes only. Additional embodiments will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein.

BRIEF DESCRIPTION OF THE DRAWINGS/FIGURES

[0009] The accompanying drawings, which are incorporated herein and form a part of the specification, illustrate embodiments of the present invention and together with the description further serve to explain the principles of the invention and to enable a person skilled in the pertinent art(s) to make and use embodiments of the invention.

[0010] Fig. 1 is a block diagram of a processor-based computing device in which embodiments of the invention may be implemented.

[0011] Fig. 2 is a flowchart illustrating a method of providing login credentials to a system implemented on a processor-based computing device according an embodiment of the invention.

[0012] Fig. 3 is flowchart illustrating a method of providing login credentials to a system implemented on a processor-based computing device according to an embodiment of the invention.

[0013] Fig. 4 is a schematic illustration of a computer-implemented system for providing login credentials to a computer system implemented according to an embodiment of the invention.

[0014] Embodiments are described below with reference to the accompanying drawings. In the drawings, like reference numbers generally refer to identical or functionally similar elements. Additionally, the leftmost digit(s) of a reference number generally identifies the drawing in which the reference number first appears.

DETAILED DESCRIPTION

[0015] This disclosure is directed to systems and methods for providing login credentials to a computer system using a biometric indicator.

[0016] It is noted that reference in this specification to "one embodiment," "an embodiment," "an example embodiment," etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but not every embodiment may necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic, is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to effect such feature, structure, or characteristic, in connection with other embodiments whether or not explicitly described.

[0017] The following detailed description refers to the accompanying drawings that illustrate exemplary embodiments consistent with this invention. The detailed description is not meant to limit the invention, but rather, the scope of the invention is defined by the appended claims.

[0018] Fig. 1 is an example computer system 100 in which embodiments of the present invention or portions thereof may be implemented as computer readable code. For example, disclosed components or modules may be implemented in one or more computer systems 100 using hardware, software, firmware, tangible computer readable media having instructions stored thereon, or a combination thereof, and may be implemented in one or more computer systems or other processing systems.

[0019] A processor-based computing device 100 can include one or more processors 102, one or more nonvolatile storage media 104, one or more memory devices 106, a communication infrastructure 108, a display device 110, and a communication interface 112. Processors 102 can include any conventional or special purpose processors including, but not limited to, digital signal processors (DSP), field programmable gate arrays (FPGA), and application specific integrated circuits (ASIC). A graphics processor unit (GPU) 114 is an example of a specialized processor that executes instructions and programs, selected for complex graphics and mathematical operations, in parallel.

[0020] A non-volatile storage device 104 can include one or more of: a hard disk, flash memory, and like devices, that can store computer program instructions and data on computer readable media. One or more of nonvolatile storage devices 104 can be a removable storage device.

[0021] Memory devices 106 can include one or more volatile memory devices such as, but not limited to, random access memory (RAM). Communications infrastructure 108 can include one or more device-interconnect buses such as Ethernet, Peripheral Component Interconnect (PCI), and the like.

[0022] Typically, computer instructions are executed using one or more processors 102 and can be stored in non-volatile storage media 104, and memory devices 106. A display screen 110 allows results of computer operations to be displayed to a user or an application developer.

[0023] A communication interface 112 allows software and data to be transferred between a computer system 100 and external devices. A communication interface 112 can include a modem, a network interface (such as an Ethernet card), a communication port, a PCMCIA slot and card or the like. Software and data transferred via a communication interface 112 can be in the form of signals, which can be electronic, electromagnetic, optical, or other signals, capable of being received by a communication interface 112. These signals can be provided to a communication interface 112 via a communications path. The communication path can carry signals and can be implemented using wire or cable, fiber optics, a phone line, a cellular phone link, an RF link, or other communications channels.

[0024] Fig. 2 illustrates a method 200 for providing login credentials to a computer system, the login credentials including a biometric indicator. In this embodiment, the biometric indicator is an image of a user requesting login access to the system. In stage 202, the system receives an image of the user. In stage 204, the image of the user that is received in stage 202 is compared with images in a database to determine whether the image matches one of the images in the database. In stage 206, a user is prompted to enter login credentials based on the comparison. In stage 208, the user is granted or denied login access based on user input entered in response to the prompting.

[0025] Fig. 3 illustrates a further embodiment method of using a biometric indicator to provide login credentials to a computer system. In stage 202, an image of the user requesting login access is received by the system. In stage 204, the image of the user requesting login access is compared with images in a database to determine whether the image matches. In stage 302, a decision is made whether or not the image matches an image in the database. If the image matches, the user is prompted in stage 304 to enter a password or passphrase. The login name of the user is automatically supplied by the system since the user's image matched a correct user in a database. In stage 308, the system receives input from the user and in stage 310 the system grants or denies access to the user based on the input received from the user in stage 308. In the event that the image does not match an image in the database in stage 302, the user is prompted in stage 306 to supply a complete set of login credentials, including a login name and password or passphrase.

[0026] Fig. 4 schematically illustrates a computer-based system 400, implemented on a processor-based computing device 100, for providing login credentials to the computer-based system using a biometric indicator. The system includes an image capture device 402, an image comparison module 406, a user interface 410, and an access control device 412. The image capture device 402 can be any device that can capture an image of a user requesting login access, such as a camera, or webcam. The image comparison module 406 is configured to compare the image of the user, captured by the image capture device 402, with a collection of images in an image database 404. The user interface 410 is configured to accept input from the image comparison module 406 and to accept user input 408 in response to prompting the user, as described above with respects to Figs. 2-3.

The access control device 412 is configured to accept input from the user interface 410 and to either grant or deny user access 414 based on the input from the user interface.

[0027] Further implementation details of exemplary systems and methods are provided in the following. In an embodiment, systems can be configured to carry out the methods described above with reference to Figs. 2 and 3, as the system is being booted up. In another embodiment, systems can be configured to capture an image of a user requesting login access after the system is already up and running.

[0028] For the first type of embodiment system, the system can be configured to load image capture software (e.g., webcam drivers) during the system boot process. Early in the boot process, after webcam drivers are loaded, an image of the user can be captured. The system can be configured to then compare the user's image against a collection of potential users to determine a possible match. The collection of potential users can include a group of users who have previously logged into the machine. Significant efficiency is gained by limiting the list of potential users to just those who have previously logged into a particular machine.

[0029] A typical user experience of such embodiment systems might be as follows. A user powers up a device, initiating a machine boot up process. When a webcam or other image capture device becomes available, it captures an image of the user. A facial recognition algorithm can then be used to compare the user's image to images of potential users in a database. As a result of the comparison, the system determines whether or not a match is found. The user is then provided with a login form containing several options. When a correct match is found the user can be prompted to enter a password. If the system determines that a match was found, but the match is incorrect, the user is provided with an opportunity to select another user. Upon selecting the correct user, a login form requesting a password would then be provided. The user would then be provided with the opportunity to enter a password. As a third option, in the situation in which no match was found or an incorrect match was found, a user would be provided with the opportunity to enter information for a new user. This third possibility might occur in the situation in which the user is logging onto the system for the first time.

[0030] As a fourth option, systems can be configured to login a user automatically. In this situation, no password is required and the user is logged in if the captured image matches an image in the database of potential users.

[0031] Embodiments may use facial recognition algorithms to compare the image of a user requesting login access with images in a database. In further embodiments, facial recognition algorithms may be used that compare key features of the image with key features of images in a database. In further embodiments, other biometric indicators may be used to identify a user, such as a retinal scanning. Other biometric indicators can also be used in embodiments to reduce the scope of potential choices for login users. Other examples include fingerprints, body heat signatures, etc.

[0032] Embodiments can also be directed to computer program products comprising software stored on any computer readable medium. Such software, when executed in one or more data processing devices, causes a data processing device to operate as described herein. Embodiments of the invention can employ any computer useable or readable medium. Examples of computer readable mediums include, but are not limited to, primary storage devices (e.g., any type of random access memory), secondary storage devices (e.g., hard drives, floppy disks, CD ROMs, ZIP disks, tapes, magnetic storage devices, optical storage devices, MEMs, nanotechnological storage devices, etc.).

[0033] Typically, computer instructions are executed using one or more processors 102 and can be stored in a non-volatile storage medium 104 or memory device 106. Computer instructions can be stored on a client or web server in a compiled file, an executable file, or a dll library. Computer instructions can also be compiled on a client prior to execution. Computer instructions can also be included in a routine, a subroutine, or layers of a software stack that are manipulated by processors 102.

[0034] Embodiments have been described above with the aid of functional building blocks illustrating the implementation of specific functions and relationships thereof. The boundaries of these functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternate boundaries can be defined so long as the specific functions and relationships thereof are appropriately performed.

[0035] The foregoing description of the specific embodiments will so fully reveal the general nature of the invention that others can, by applying knowledge within the skill of the art, readily modify and/or adapt for various applications, such specific embodiments without undue experimentation, without departing from the general concept of the present invention. Therefore, such adaptations and modifications are intended to be within the meaning and range of equivalents of the disclosed embodiments based on the teachings and guidance presented herein. It is to be understood that the phraseology or terminology herein is for the purpose of description and not of limitation, such that the terminology or phraseology of the present specification is to be interpreted by the skilled artisan in light of the teaching and guidance presented herein.

[0036] The Summary and Abstract sections may set forth one or more but not all exemplary embodiments of the present invention as contemplated by the inventors, and thus, are not intended to limit the present invention and appended claims in any way.

[0037] The breadth and scope of the present invention should not be limited by any of the above described exemplary embodiments, but rather, should be defined only in accordance with the following claims and their equivalents.

WHAT IS CLAIMED IS:

1. A computer implemented method, comprising:

receiving, by a computational device, an image of a user requesting login access to a client device;

comparing, by the computational device, the image with images of authorized users in a database to determine whether the image matches an image in the database;

prompting the user to enter login credentials based on the comparing, wherein the prompting comprises requesting the user to enter one of the following based on the result of the comparing:

a reduced set of login credentials when a correct match is found; or

a complete set of login credentials when no match is found or when an incorrect match is found; and

granting or denying the user login access based on the login credentials entered by the user.

2. The method of claim 1, wherein the prompting comprises requesting the user to confirm or deny that a correct match has been found.

3. The method of claim 1, wherein the comparing comprises using a facial recognition algorithm to compare the image with images in a database.

4. The method of claim 3, wherein the comparing comprises using a facial recognition algorithm to compare key features of the image with key features of images in a database.

5. The method of claim 1, further comprising:

granting the user login access when a complete set of login credentials is entered that correspond to an authorized user;

granting the user login access when a reduced set of login credentials is entered that corresponds to the authorized user whose image in the data base was matched by the image of the user that is requesting login access; or

denying the user login access otherwise.

6. A computer readable storage medium having program instructions stored thereon that, when executed by a processor, cause the processor to grant or deny login access, the program instructions comprising computer readable code that causes a computer to:

receive an image of a user requesting login access to a client device;

compare the image with images of authorized users in a database to determine whether the image matches an image in the database;

prompt the user to enter login credentials based on the comparing, wherein the prompting comprises requesting the user to enter one of the following based on the result of the comparing:

a reduced set of login credentials when a correct match is found; or

a complete set of login credentials when no match is found or when an incorrect match is found; and

grant or deny the user login access based on the login credentials entered by the user.

7. The computer readable storage medium of claim 6, wherein the program instructions further comprise computer readable code that causes the computer to prompt the user to confirm or deny that a correct match has been found.

8. The computer readable storage medium of claim 6, wherein the program instructions further comprise computer readable code that causes the computer to use a facial recognition algorithm to compare the image with images in a database.

9. The computer readable storage medium of claim 8, wherein the program instructions further comprise computer readable code that causes the computer to use a facial recognition algorithm to compare key features of the image with key features of the images in a database.

10. The computer readable storage medium of claim 6, wherein the program instructions further comprise computer readable code that causes the computer to:

grant the user login access when a complete set of login credentials is entered that correspond to an authorized user;

grant the user login access when a reduced set of login credentials is entered that corresponds to the authorized user whose image in the data base was matched by the image of the user that is requesting login access; or

deny the user login access otherwise.

11. A computer implemented system, comprising:

an image comparison module configured to compare an image of a user requesting login access to a client device, with images in a database to determine whether the image matches an image in the database;

a user interface configured to receive input from the image comparison module and to prompt the user for login credentials based on the input received from the comparison module, wherein the prompting comprises requesting the user to enter one of the following based on the result of the comparing:

a reduced set of login credentials when a correct match is found; or

a complete set of login credentials when no match is found or when an incorrect match is found; and

an access control module configured to grant or deny the user login based on user input that is entered in response to the prompting.

12. The system of claim 11, wherein the user interface is further configured to prompt the user to confirm or deny that a correct match has been found.

13. The system of claim 11, wherein the image comparison module is further configured to use a facial recognition algorithm to compare the image with images in the database.

14. The system of claim 13, wherein the image comparison module is further configured to use a facial recognition algorithm to compare key features of the image with key features of images in the database.

15. The system of claim 11, wherein the image comparison module is further configured to update image comparison criteria based on user input when an incorrect match is found.

16. The system of claim 11, wherein the access control module is further configured to:

grant the user login access when a complete set of login credentials is entered that correspond to an authorized user;

grant the user login access when a reduced set of login credentials is entered that corresponds to the authorized user whose image in the data base was matched by the image of the user that is requesting login access; or

denying the user login access otherwise.

17. The system of claim 11, further comprising an image capture device that is configured to capture an image of the user as part of the system boot process.

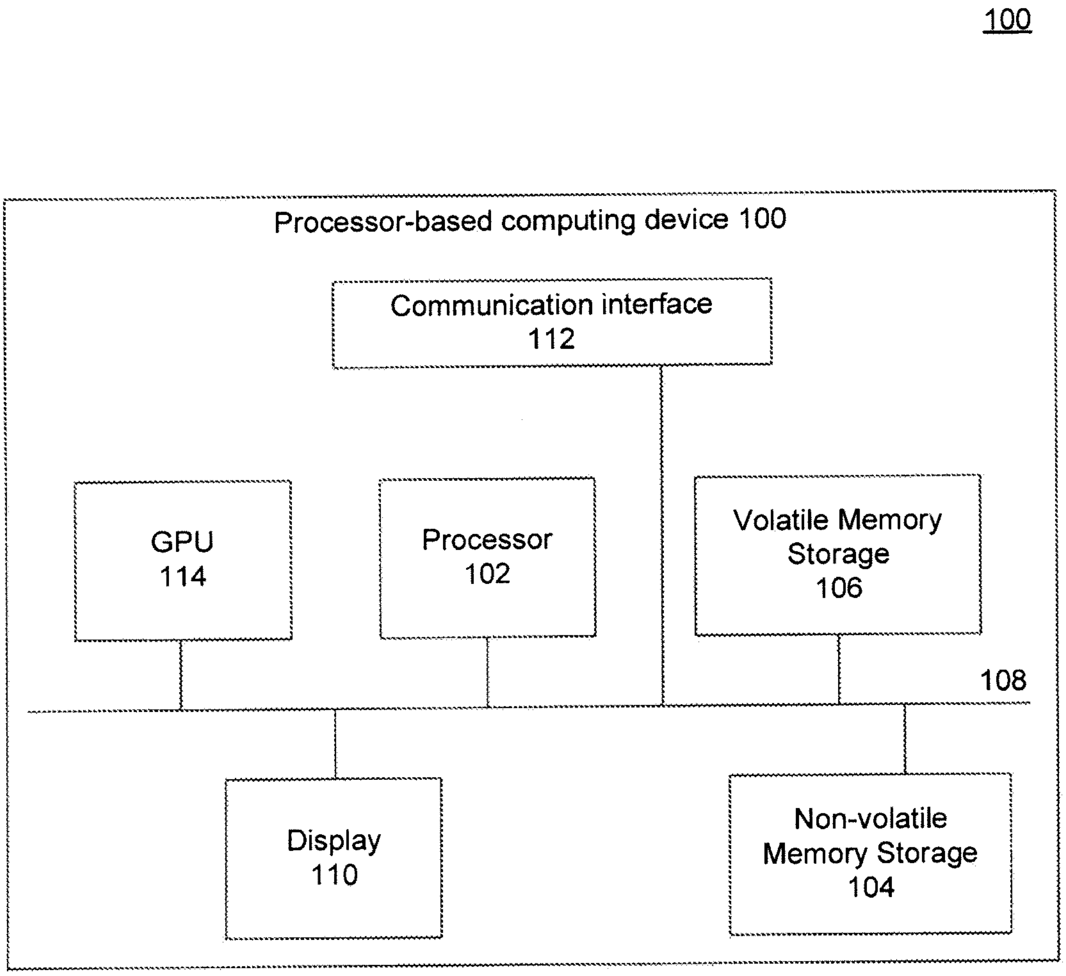

100
Processor-based computing device 100
Communication interface 112
GPU 114
Processor 102
Volatile Memory Storage 106
108
Display 110
Non-volatile Memory Storage 104

FIG. 1

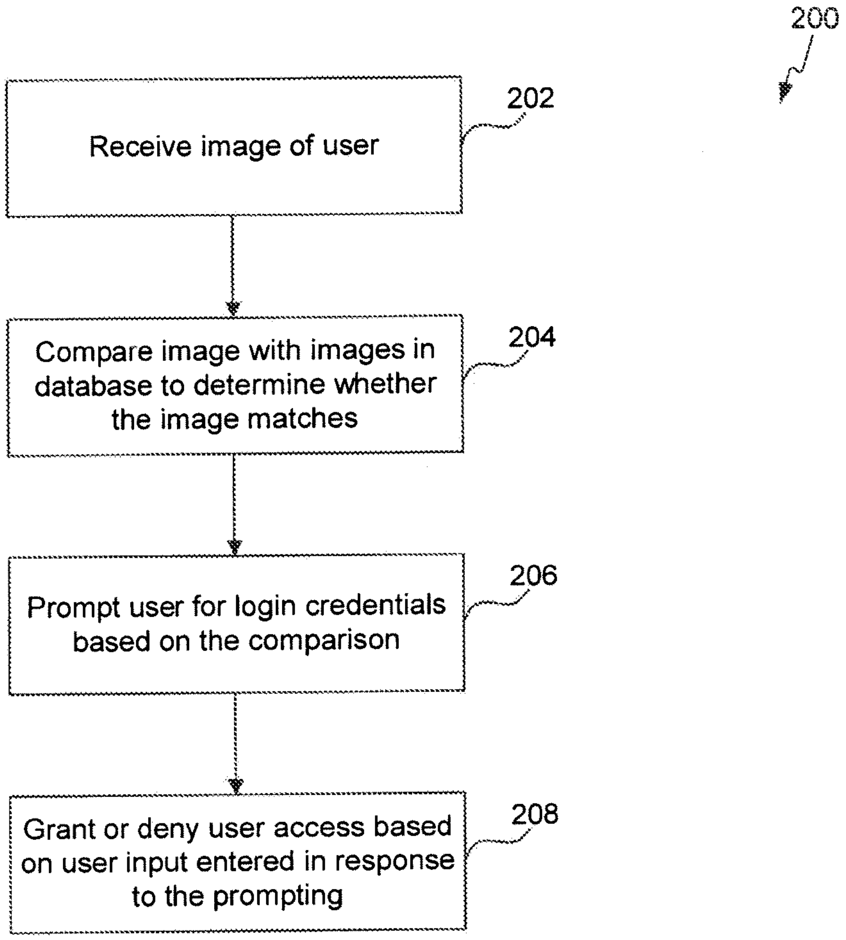

200
Receive image of user
202
Compare image with images in database to determine whether the image matches
204
Prompt user for login credentials based on the comparison
206
Grant or deny user access based on user input entered in response to the prompting
208

FIG. 2

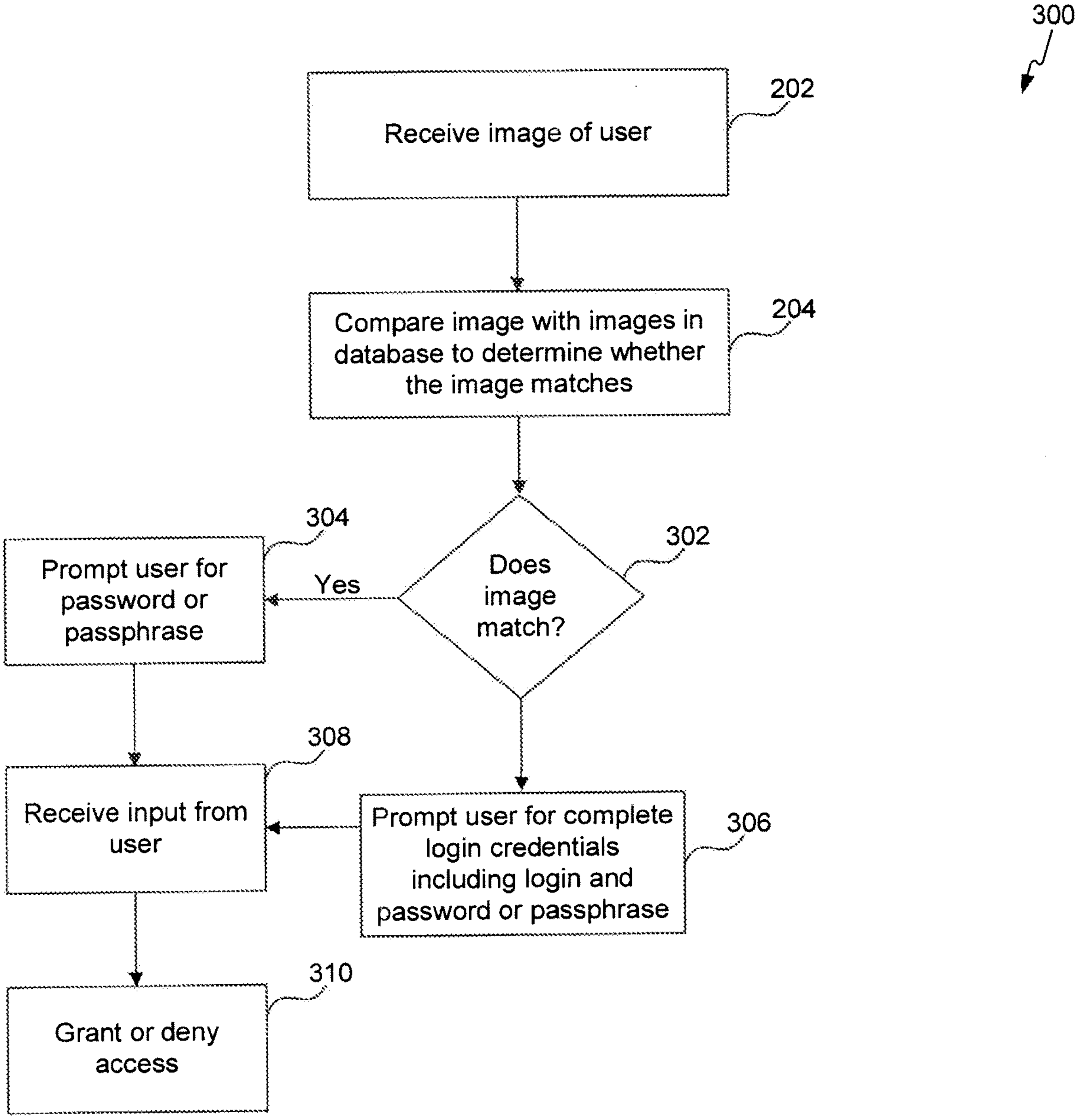

300
Receive image of user
202
Compare image with images in database to determine whether the image matches
204
Does image match?
302
Yes
Prompt user for password or passphrase
304
Receive input from user
308
Prompt user for complete login credentials including login and password or passphrase
306
Grant or deny access
310

FIG. 3

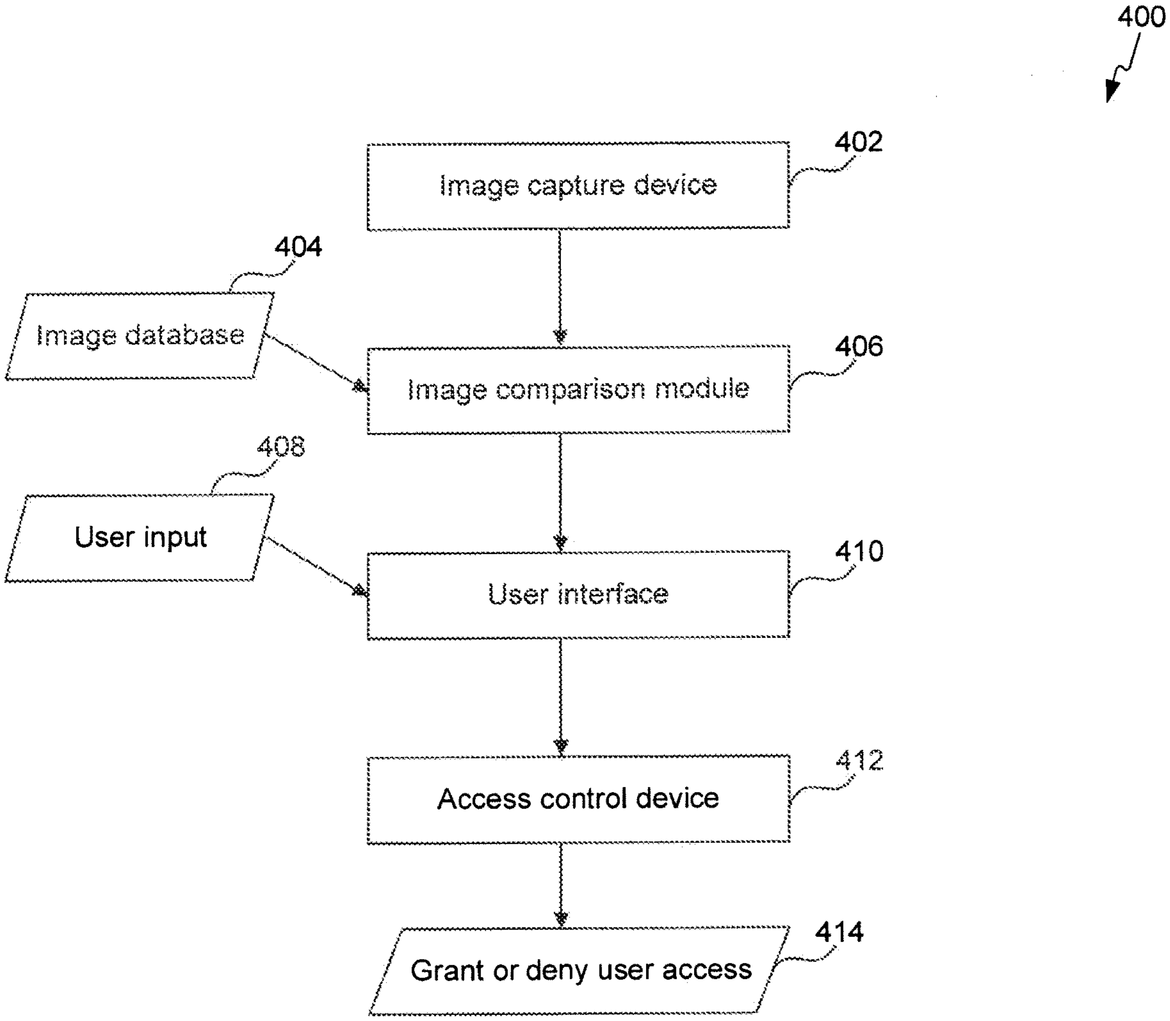

400
Image capture device
402
Image database
404
Image comparison module
406
User input
408
User interface
410
Access control device
412
Grant or deny user access
414

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/023302

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/32(2013.01)i

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)
G06F 21/32; G06F 3/048; H04K 1/00; G06F 21/20; G06F 17/30; G06Q 50/10; G06K 9/00; G06F 21/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: login, image, facial, match, database, credential, authorize, camera, comparison, algorithm

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006-0288234 A1 (CYRUS AZAR et al.) 21 December 2006 See paragraphs 2-4, 18-21; claim 41; and figures 1-3.	1-14,16-17
Y		15
Y	US 2009-0252383 A1 (HARTWIG ADAM et al.) 08 October 2009 See paragraphs 63-67; and figure 1.	15
A	US 2011-0206244 A1 (CARLOS MUNOZ-BUSTAMANTE) 25 August 2011 See paragraphs 23, 29, 31-33; and figures 1-3.	1-17
A	US 2009-0077653 A1 (STEVEN L. OSBORN et al.) 19 March 2009 See paragraph 23; and figures 1-2.	1-17
A	KR 10-2011-0103676 A (DGM IT CO,.LTD.) 21 September 2011 See paragraphs 6, 11-21; and figures 1-2.	1-17
A	KR 10-2010-0010180 A (MIRAE RECOGNITION CO.,LTD.) 01 February 2010 See paragraphs 5-6, 8; and figures 1-2.	1-17

□ 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 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 09 July 2013 (09.07.2013)	Date of mailing of the international search report **10 July 2013 (10.07.2013)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. +82-42-472-7140	Authorized officer BYUN Sung Cheal Telephone No. +82-42-481-8262

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2013/023302

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006-0288234 A1	21/12/2006	US 2009-0251560 A1	08/10/2009
		US 2013-114865 A1	09/05/2013
		US 8189096 B2	29/05/2012
		US 8370639 B2	05/02/2013
		WO 2007-055745 A2	18/05/2007
		WO 2007-055745 A3	23/04/2009
US 2009-0252383 A1	08/10/2009	CN 101990667 A	23/03/2011
		EP 2281248 A1	09/02/2011
		JP 2011-516966 A	26/05/2011
		KR 10-2010-0129783 A	09/12/2010
		US 8358811 B2	22/01/2013
		WO 2009-123711 A1	08/10/2009
US 2011-0206244 A1	25/08/2011	None	
US 2009-0077653 A1	19/03/2009	None	
KR 10-2011-0103676 A	21/09/2011	None	
KR 10-2010-0010180 A	01/02/2010	None	