

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
20 October 2005 (20.10.2005)

PCT

(10) International Publication Number
WO 2005/096768 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2005/011518

(22) International Filing Date: 6 April 2005 (06.04.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/559,804 6 April 2004 (06.04.2004) US

(71) Applicant (for all designated States except US): **RF INTELLIGENT SYSTEMS, INC.** [US/US]; 12954 Park Crescent Circle, Oak Hill, Virginia 20171 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **SIM, Michael L.** [GB/US]; 1724 Lake Shore Crest Drive #13, Reston, Virginia 20190 (US).

(74) Agent: **ROBINSON, Melvin A.**; Patent Department, Schiff Hardin LLP, 6600 Sears Tower, Chicago, Illinois 60606 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

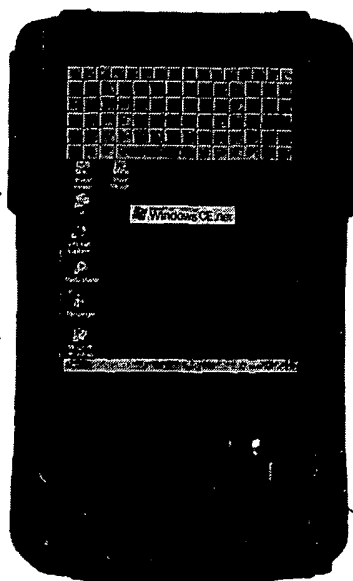
Declarations under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA,

[Continued on next page]

(54) Title: COMBINED 2D/3D FACIAL AUTHENTICATION

- g) 802.11 WLAN
OPTION * →
- e) EMBEDDED
RFID READER * →
- f) EMBEDDED
SMARTCARD
READER * →



RELEASE VERSION

- a) MINIATURE SCAN ENGINE = TWIN IMAGER
TO ACHIEVE 3D IMAGE AND BARCODE
- b) TOUCH CHIP FINGERPRINT
- c) IR LED
- d) STANDARD LED
- e) EMBEDDED RFID
- f) SMARTCARD READER
- g) 802.11 WLAN GPRS OPTION

* Optional Extras

(57) Abstract: A method and apparatus for authenticating an identification of a person includes a device to capture two dimensional and three dimensional data. Both 2D and 3D biometric data are stored on a data carrier to be provided to a person to be identified. The biometric data on the data carrier is compared to biometric data obtained from the person and if a match is made then the identity is authenticated.



MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

S P E C I F I C A T I O N

"COMBINED 2D / 3D FACIAL AUTHENTICATION"

5

CROSS-REFERENCE TO RELATED APPLICATION

[0001] The present application claims the benefit of Provisional Patent Application
10 Serial No. 60/559, 804, filed April 6, 2004, which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

Field of the Invention

[0002] The present invention relates generally to a method and apparatus for
15 identification of a person and in particular to a method and apparatus for authenticating an
identification.

Description of the Related Art

[0003] Biometrics is the science of automatically identifying individuals based on
their unique physiological and behavioral characteristics. Biometric information may be
20 based on unique characteristics of a person's face, iris, voice, fingerprint, signature or DNA.
These identification techniques can all be used to authenticate a person's identity from
information stored in a database or held on a token as a two dimensional barcode, magnetic
stripe, smart card, USB (Universal Serial Bus) device, memory stick or RFID (Radio
Frequency Identification) format device.

25 [0004] The use of facial recognition has advantages over and above those of other
biometrics, particularly in that the process is non-intrusive. Until recently this process was
limited to the person being in front of a camera. The advent of handheld wireless technology
now allows migration of the recognition process to remote or difficult environments.

[0005] Identification systems are disclosed in International Patent Application
30 publications WO 00/62474 published October 19, 2000, and WO 02/09024 A1 published on

January 31, 2002. In WO 00/62474, a computer uses a facial biometric template to encode a document. In WO 02/09024 A1, a facial identification matrix is obtained. 2D and 3D biometric templates are created from a single camera and the facial index data is extracted. These published applications are incorporated herein by reference.

5

SUMMARY OF THE INVENTION

[0006] The present invention provides a method and apparatus using a combination of two dimensional and three dimensional biometric template data to authenticate an identification.

BRIEF DESCRIPTION OF THE DRAWINGS

10 [0007] **Figure 1** is a schematic front view of a portable identification device having a fingerprint sensor;

[0008] **Figure 2** is a schematic review view of the portable identification device of **Figure 1** having dual imaging devices;

15 [0009] **Figure 3** is a top plan view of the portable identification device according to the preferred embodiment of the invention;

[0010] **Figure 4** is a functional block diagram of an enrollment process performed by the present identification device;

[0011] **Figure 5** is a functional block diagram of an authentication process performed by the identification device; and

20 [0012] **Figure 6** is a functional block diagram of hardware and software definition for the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0013] In Figure 1 is shown schematically an identification module 10 having a rugged housing and a touch pad fingerprint sensor 12. The fingerprint sensor 12 is used to obtain fingerprint biometric data.

5 [0014] In Figure 2, the other end of the identification module 10 is shown. The module has two camera lenses 14 and imaging devices facing the same direction and spaced apart by a predetermined distance. The imaging devices are electronic imaging devices, such as CCD or CMOS imaging devices. Other types of imaging chips may be provided as well. Both imaging devices are operated at the same time to take two images spaced by the
10 predetermined distance. Thus, the imaging devices obtain a stereographic image that includes three dimensional information of the object being imaged.

[0015] Proper illumination is important during imaging using the electronic imaging system. The illumination is provided here by a ring shaped lighting system 16 surrounding each lens. The ring shaped lighting system 16 of a preferred embodiment has a plurality of
15 LEDs in each ring. The LEDs are of two types. First, five visible light LEDs 18 are provided in the ring light system and, second, five IR (InfraRed) LEDs 20 are provided in each ring light system. Thus, each ring light system includes ten LEDs to provide illumination to the subject being imaged. To ensure that the infrared energy from the IR LEDs is effective in illuminating the subject, the imaging chip (either CCD or CMOS) does not have an IR filter.
20 Such IR filters are common in commercial imaging systems, such as digital cameras and will not be provided here. The lighting system can use either the visible light, the infrared light or both in obtaining the stereographic images.

[0016] The stereographic images are input to software to generate two dimensional and three dimensional biometric information about a subject. The biometric information is
25 combined. This information is stored on a data carrier that is provided to a person that has been identified. The data carrier is any of a variety of data carriers, which are referred to as a token, card, or the like.

[0017] Combined 2D/3D facial biometric template data is read from a token, storage media or other data carrier and compared to live 3D images captured via a ruggedly built handheld computer identification device. The computer identification device is shown in **Figure 3**. Simultaneous images are sent wirelessly to a central server where software stitching is performed to produce a single 3D image. The 3D image is converted via software to a 3D biometric template. The newly generated template is compared to 3D facial biometric data that is held in the storage media. At the same time, an extraction process is performed on the 3D image to extract 2D biometric data from the 3D image. The extracted 2D data is compared to 2D biometric data extracted from the storage media. (See Figures 4 and 5 relating to an enrollment process for recording biometric information from an identified person and an authentication process for authenticating the identity of a person to be identified).

[0018] The combination of these two methods results in an authentication (level of match) score being displayed on the handheld computer. Authentication levels can be adjusted up or down depending on a level of security required. The handheld computer operator has the facility to interrogate the score and review either the 2D or 3D results, or both, should there be a discrepancy in the overall results. The operator can also call up and display the original photo image stored at the time of enrollment for additional visual confirmation.

[0019] As shown in **Figure 4**, an enrollment process proceeds as follows: The enrollment is achieved using either a ruggedly built handheld computer with a twin image capture apparatus or by a 3D (three dimensional) camera connected to a PC. In the case of the handheld computer, two separate image streams are fed simultaneously to a server via a wireless communication, in the preferred embodiment, which communication can include communications according to the 802.11b standard, WLAN (Wireless Local Area Network), GPRS (General Packet Radio Service) or CDMA (Code Division Multiple Access). 3D (three dimensional) software is resident on the server to receive the image data. A 3D software process combines the incoming video feeds to produce a live 3D (three dimensional)

image. The 3D software then extracts a 3D template. At the same time combined 2D (two dimensional) software extracts a 2D template from the same 3D image source.

[0020] Storage of the identification data is carried out as follows. Both templates are individually processed to extract key biometric data for storage in a two-dimensional barcode, magnetic stripe, RFID (Radio Frequency Identification), USB (Universal Serial Bus) token or chip format. (See **Figure 4**). The residual template information is tagged with a multiple digit identification number and stored on the server.

[0021] Referring to **Figure 5**, an authentication process is carried out as follows. At the time of authentication, the stored template (key) information is read from the card or token. Using the handheld computer, twin images are fed to the server. Both 3D and 2D templates are then extracted from the live feed for comparison with the previously stored card information and the residual template information held on the server. The two scores are then combined and transmitted back to the handheld computer and displayed as a level of confidence in the match. The handheld computer operator can call up either the 3D or 2D information if required. Also at this time the original image taken at the time of enrollment is displayed. (See **Figure 4**).

[0022] The biometric information may be updated according to the follows process. As part of the authentication process, the stored template information can be updated seamlessly, if the authentication levels drop below a preset threshold. Re-writable token media can be updated seamlessly whereas in the case of two dimensional barcode ID there would be a need to reprint.

[0023] In **Figure 6**, a control apparatus is connected to the two cameras and a fingerprint sensor as inputs. A control for the lighting is provided. A display is connected to the control through a device controller. Data input to the device is possible through a card reader or radio frequency device reader. Image capture and processing software provides 2D and 3D processing, 3D capture and iris identification. A communications port through a

wireless TCP/IP connection, for example, provides data to and from a server or other network.

[0024] The identification accuracy can be increased. The use of two separate facial biometric processes significantly increases the overall accuracy of the authentication when measured against either of the biometric methods used individually. Similar improvements in accuracy can be achieved by combining either the 2D/3D facial with fingerprint or other biometric data.

[0025] Thus, there is shown and described a method for producing both 2D and 3D facial biometric authentication from a single 3D image capture process. In the preferred embodiment, a capture of 2D and 3D facial biometrics is achieved with a rugged handheld computer. The overall accuracy of the authentication process is substantially improved by combining two separate algorithms.

[0026] Facial biometrics includes more than just surface features of the face. It includes iris, wrinkling, scarring, wounds, tattoo (and tattoo removal) patterns and features including subdermatological patterns, pores and other dermatological depth and variation, hair features such as thickness, baldness patterns as well as hair chemical composition, ears, teeth cavity and tooth growth patterns/dentures/gums and other features internal to the face including the mouth, nose and eyes, ears external and internal to the body, coloring, cranial and bone structure and pattern, internal anatomy, brain features, brain activity, pheromone (i.e., various odors of the person or object), salinity and chemical patterns, body temperature, motion patterns such as a specific tick or Parkinson's type shake, walking limp, nervous habit (such as scratching, tapping, knee-shaking), aura-type variations, and other features and characteristics. All of these features and characteristics can be detected and captured non-invasively as well. These are all included within the scope of the invention.

[0027] With the foregoing in mind, the identification and authentication method and system includes linked databases that might separately contain information on any one, or more than one, such feature named above. For example, the mobile device can include

identification and authentication of bar coded or other stored information in more than one database. These multiple databases might include iris identification in one database and other facial identification in a second, third or more databases.

[0028] Various databases are in existence today and more are coming on-line that will have pieces of this type of biometric information – hospital records might have a cranial and brain scan MRI, dental records might have a full jaw, iris may be captured by an “agency” information database, states have pictures on licensing databases, etc. The present invention is capable of linking to and utilizing more than one database in the detection and authentication method and system.

[0029] The present system and method is designed not only to operate in normal (e.g., daylight, laboratory, good weather condition at sea level, at one atmosphere, etc) conditions. The system is mobile so that it will be utilized in a wide range of environments. These include space programs, subterranean, underwater, sea water/fresh water/brine water, excessive heat and cold, and under compromised or chemical/radiological environments including bio hazardous environments that present imperfect conditions. As such, the ruggedly built housing and the components are selected and constructed to withstand these harsh environmental conditions and so permit operation of the device wherever needed.

[0030] Not only is the system and method designed to be able to identify and authenticate in these environments as noted above, but also the method or system is designed so that it can function completely within its own ruggedized housing or enclosure. For example, a normal PDA or blackberry or the like will not function as intended in extreme environments noted above. The present device, by contrast, includes a system or method that can operate under the harsh/abnormal environment including wet (sea/fresh/brine water), hot/cold temperature conditions; chemically or radiologically- or biologically-tainted or compromised environment; excessive dust/dirt (including desert-type), wind, pressure and vibration environments.

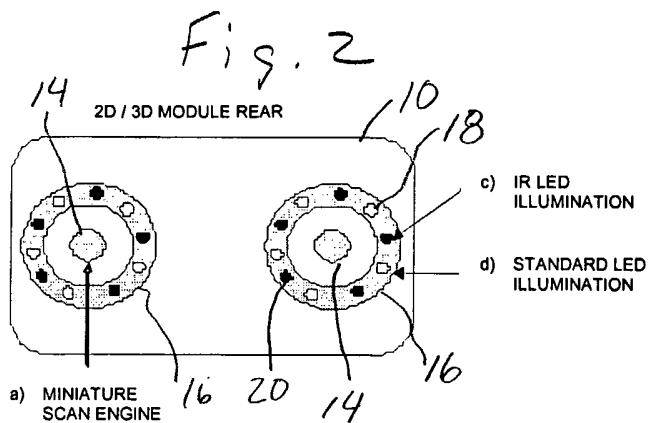
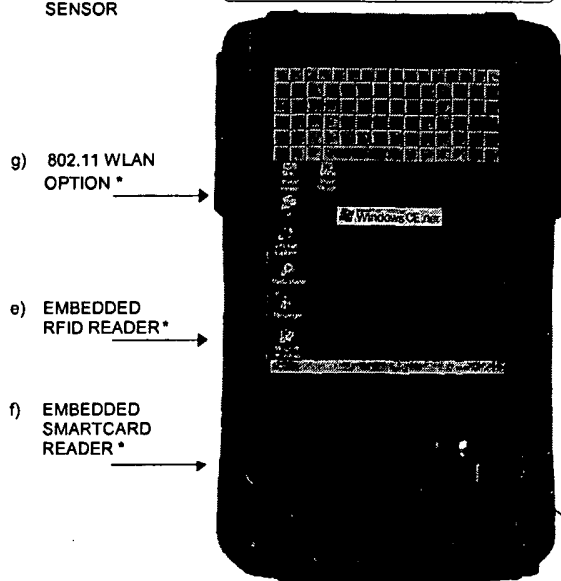
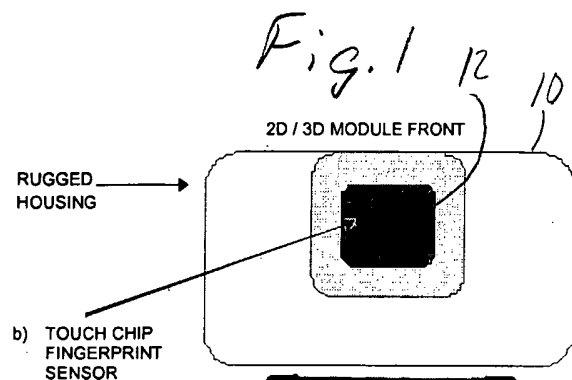
[0031] The present application is related to the subject matter of co-pending United States Provisional Patent Applications Serial No. 60/559,883 filed April 6, 2004, Serial No. 60/559,933 filed April 6, 2004, and Serial No. 60/559,805 filed April 6, 2004, and to the non-provisional applications claiming the benefit thereof. All of these applications are

5 incorporated herein by reference.

[0032] Although other modifications and changes may be suggested by those skilled in the art, it is the intention of the inventors to embody within the patent warranted hereon all changes and modifications as reasonably and properly come within the scope of their contribution to the art.

I CLAIM:

1. A method for authenticating an identification, comprising the steps of:
obtaining a three dimensional image of an identified person;
generating two dimensional biometric information from the three dimensional image;
5 storing the two dimensional biometric information and the three dimensional image of the
person in an identification system;
obtaining a three dimensional image of a person to be identified;
generating two dimensional biometric information from the three dimensional information of
the person to be identified; and
10 comparing the two dimensional biometric information of the person to be identified to the
two dimensional biometric information of the identified person and comparing the
three dimensional image information of the person to be identified to the three
dimensional image information of the person to be identified, a result of said
comparing step providing a potential authentication of an identification of the person
15 to be identified.



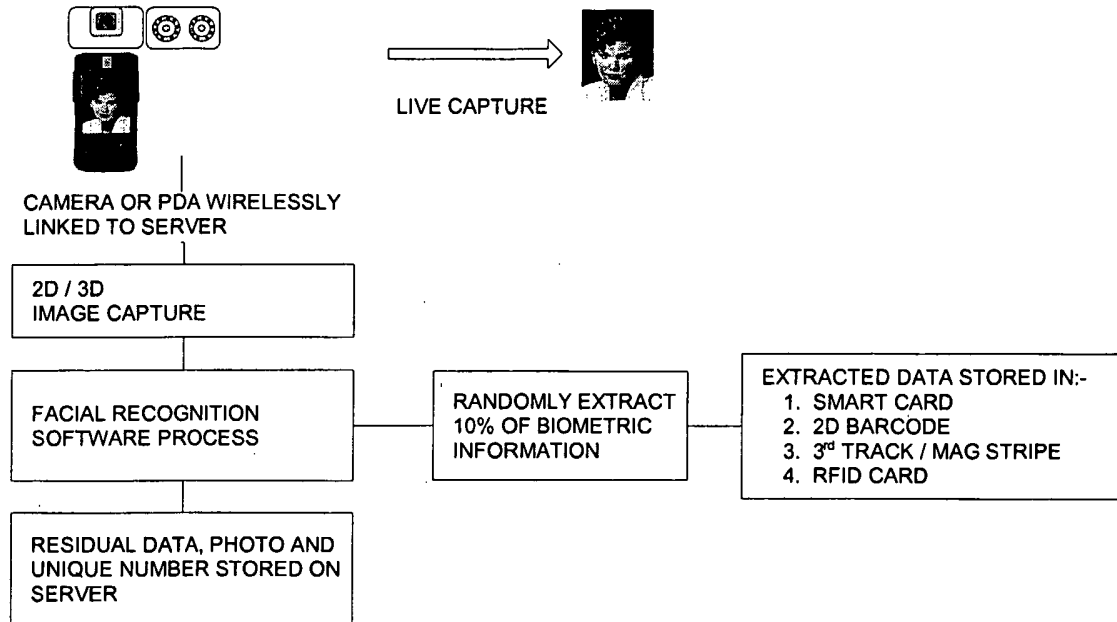
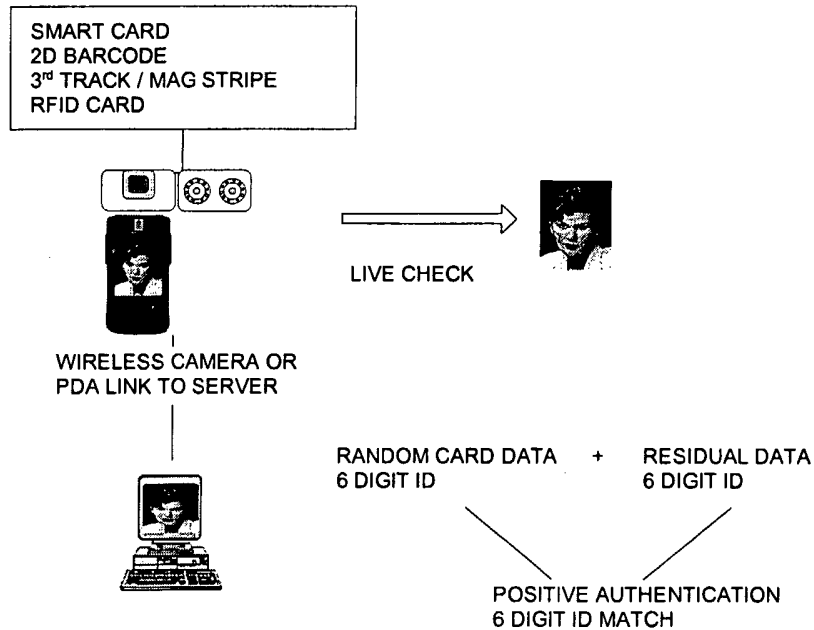
RELEASE VERSION

- a) MINIATURE SCAN ENGINE = TWIN IMAGER TO ACHIEVE 3D IMAGE AND BARCODE
- b) TOUCH CHIP FINGERPRINT
- c) IR LED
- d) STANDARD LED
- e) EMBEDDED RFID *
- f) SMARTCARD READER
- g) 802.11 WLAN GPRS OPTION

* Optional Extras

Fig. 3

Fig. 4

ENROLMENT PROCESS**AUTHENTICATION PROCESS**

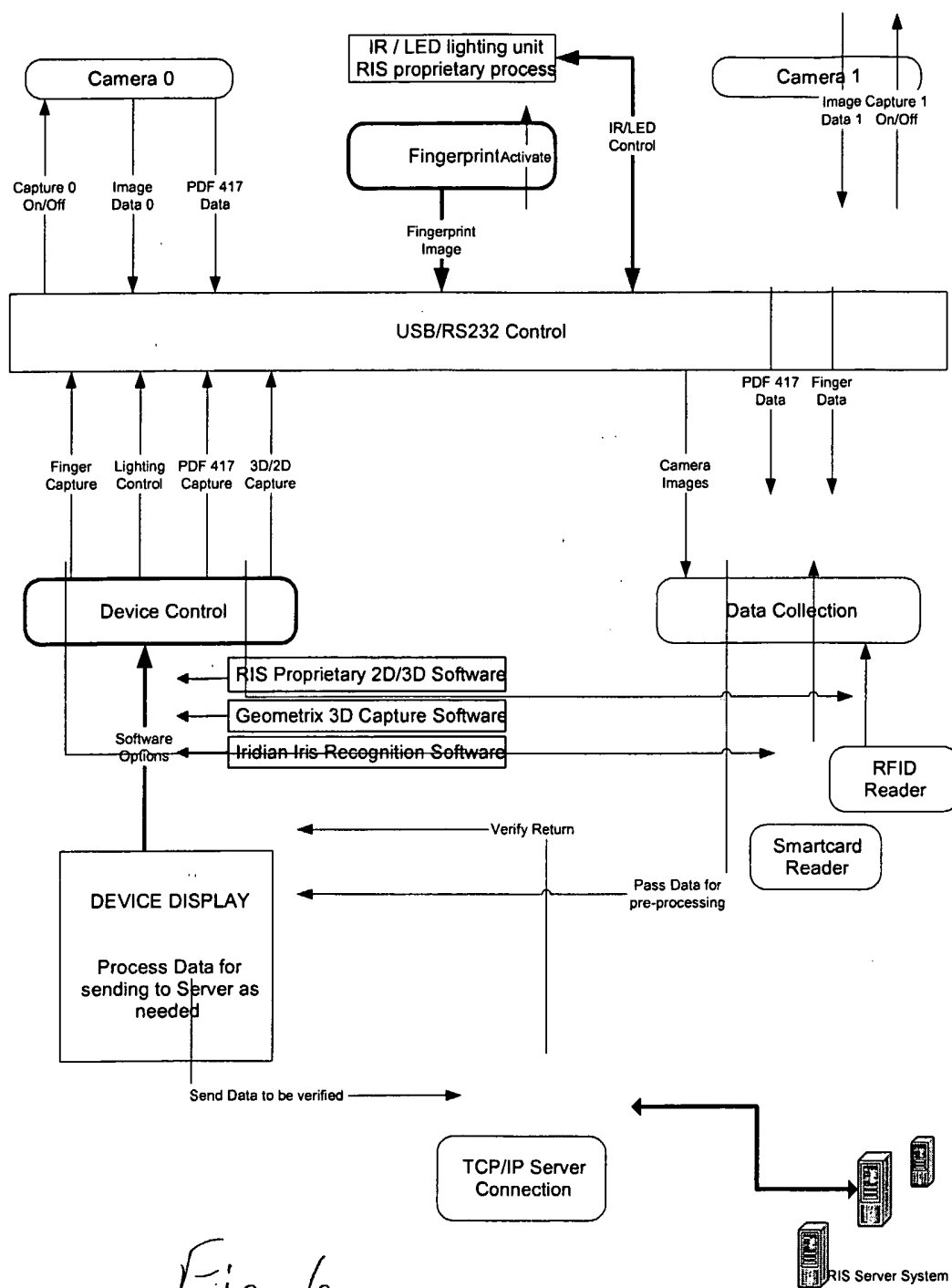


Fig. 6