US 20050264398A1

(19) **United States**

(12) **Patent Application Publication**

Siegel et al.

(10) **Pub. No.: US 2005/0264398 A1**

(43) **Pub. Date: Dec. 1, 2005**

(54) **SYSTEMS AND METHODS UTILIZING BIOMETRIC DATA**

(75) Inventors: **William G. Siegel**, Wellington, FL (US); **Gregory L. Cannon**, Boynton Beach, FL (US)

Correspondence Address:
STERNE, KESSLER, GOLDSTEIN & FOX PLLC
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005 (US)

(73) Assignee: **Cross Match Technologies, Inc.**, Palm Beach Gardens, FL

(21) Appl. No.: **11/099,697**

(22) Filed: **Apr. 6, 2005**

Related U.S. Application Data

(63) Continuation of application No. 10/125,650, filed on Apr. 19, 2002.

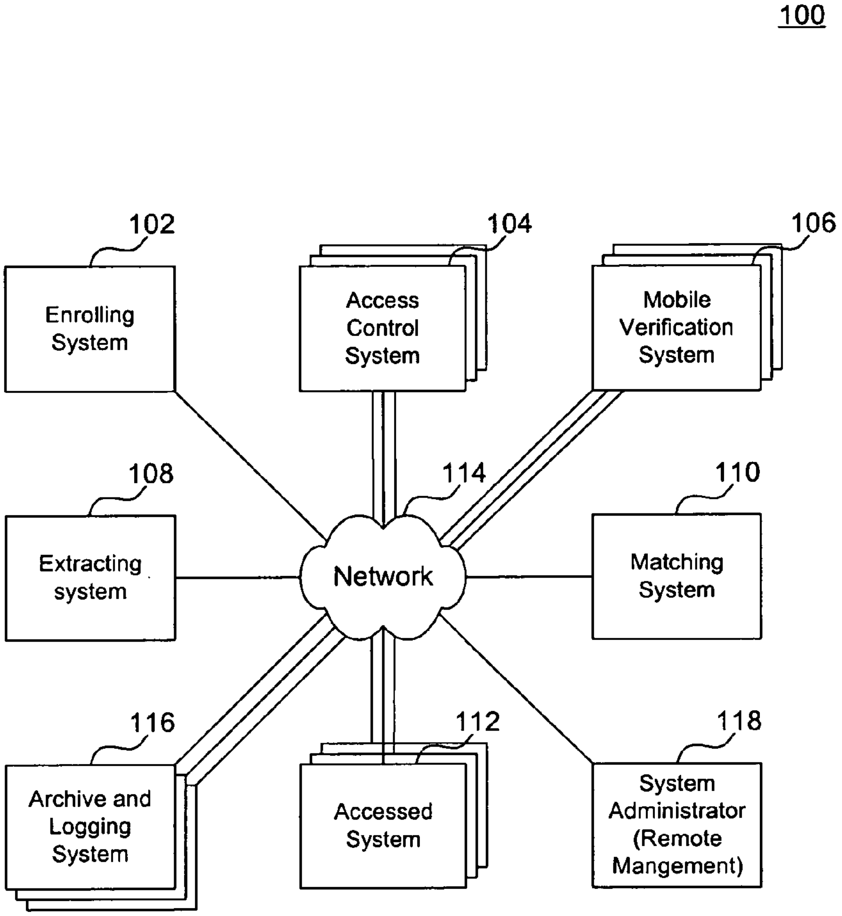
Publication Classification

(51) **Int. Cl.^{7}** **G06F 7/00**

(52) **U.S. Cl.** **340/5.52**

(57) **ABSTRACT**

Systems and methods perform access control and mobile identity verification utilizing a memory, maybe on a handheld device, that stores at least biometric data, such as minutia. The handheld device may also store other data, such as a threshold value and Wiegand data. The data may be stored in a memory, a magnetic strip, a code, a bar code, or in all of these devices associated with the handheld device. The handheld device may be a SmartCard or the like. The threshold value may be a required value or parameter generated from input criteria based on biometric data read and extracted by an extracting system during an enrolling process. The threshold value is used during extracting, matching, or both, to most accurately determine the identity and characteristics of an individual wanting access to an accessed system or being questioned by law enforcement in the field.



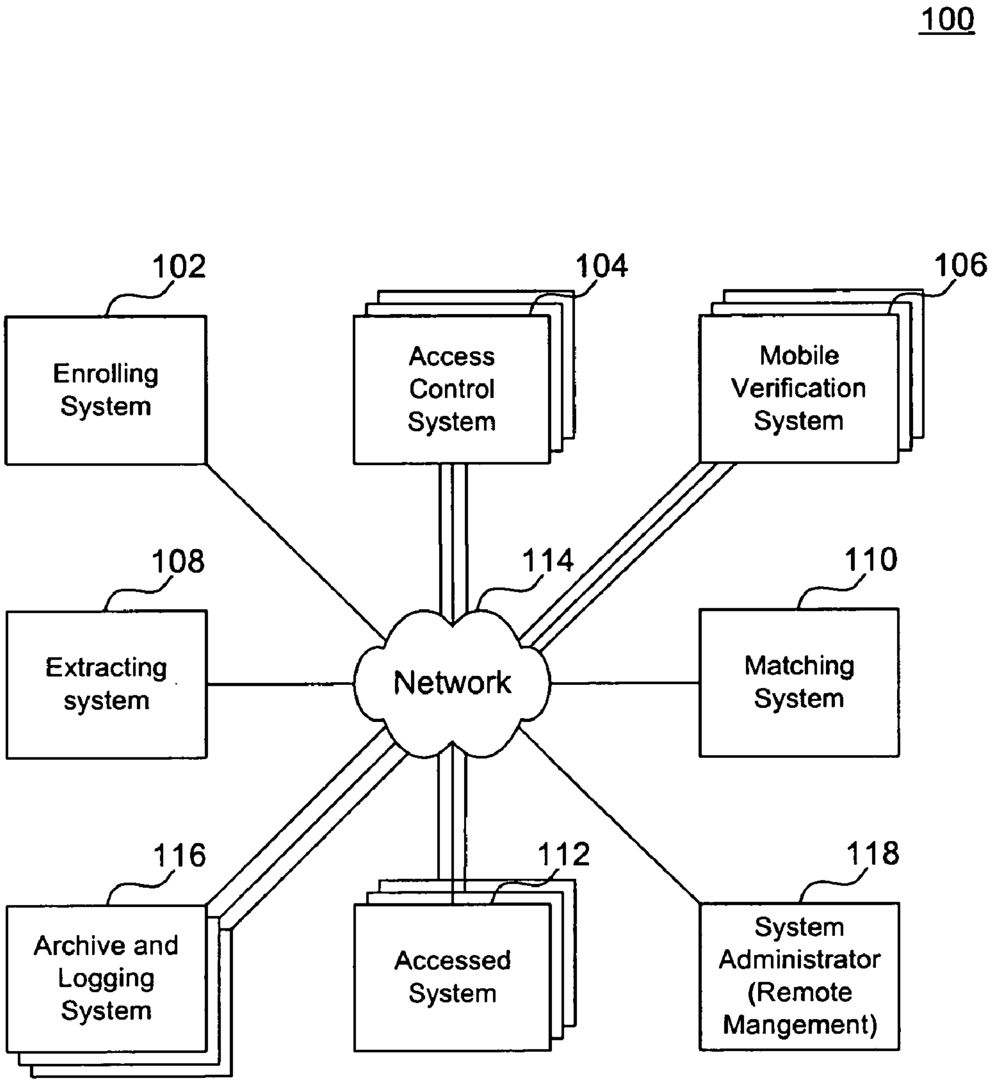

100
102
Enrolling System
104
Access Control System
106
Mobile Verification System
108
Extracting system
114
Network
110
Matching System
116
Archive and Logging System
112
Accessed System
118
System Administrator (Remote Mangement)

FIG. 1

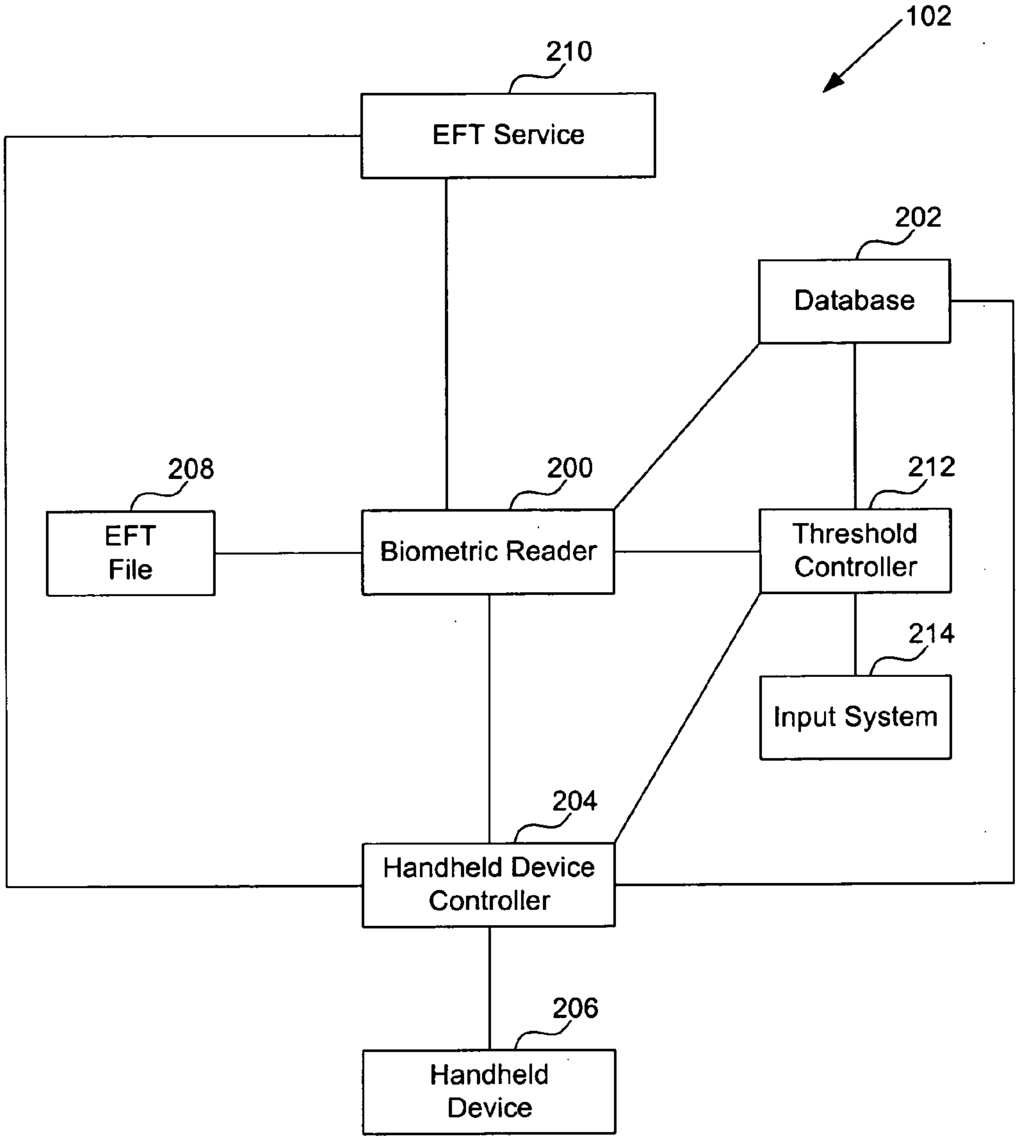

102
210
EFT Service
202
Database
208
EFT File
200
Biometric Reader
212
Threshold Controller
214
Input System
204
Handheld Device Controller
206
Handheld Device

FIG. 2

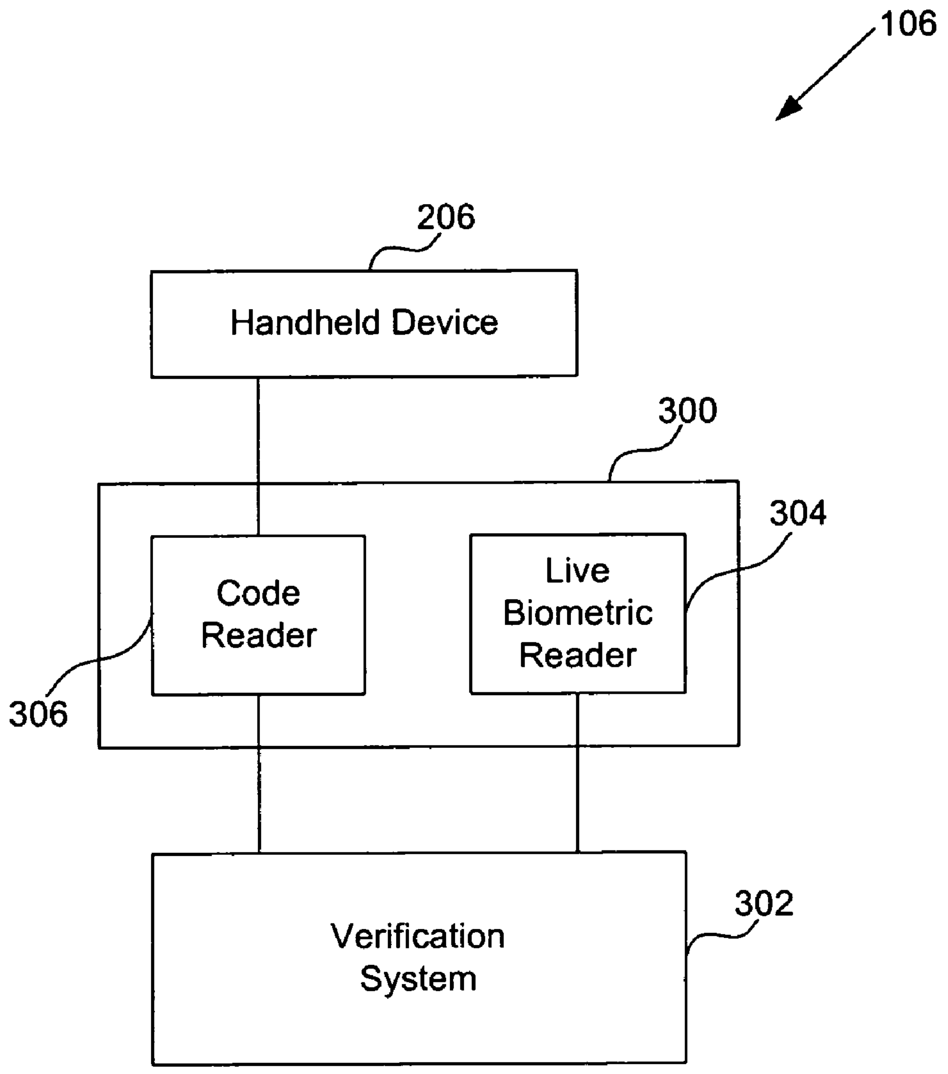

106
206
Handheld Device
300
304
Code Reader
Live Biometric Reader
306
Verification System
302

FIG. 3

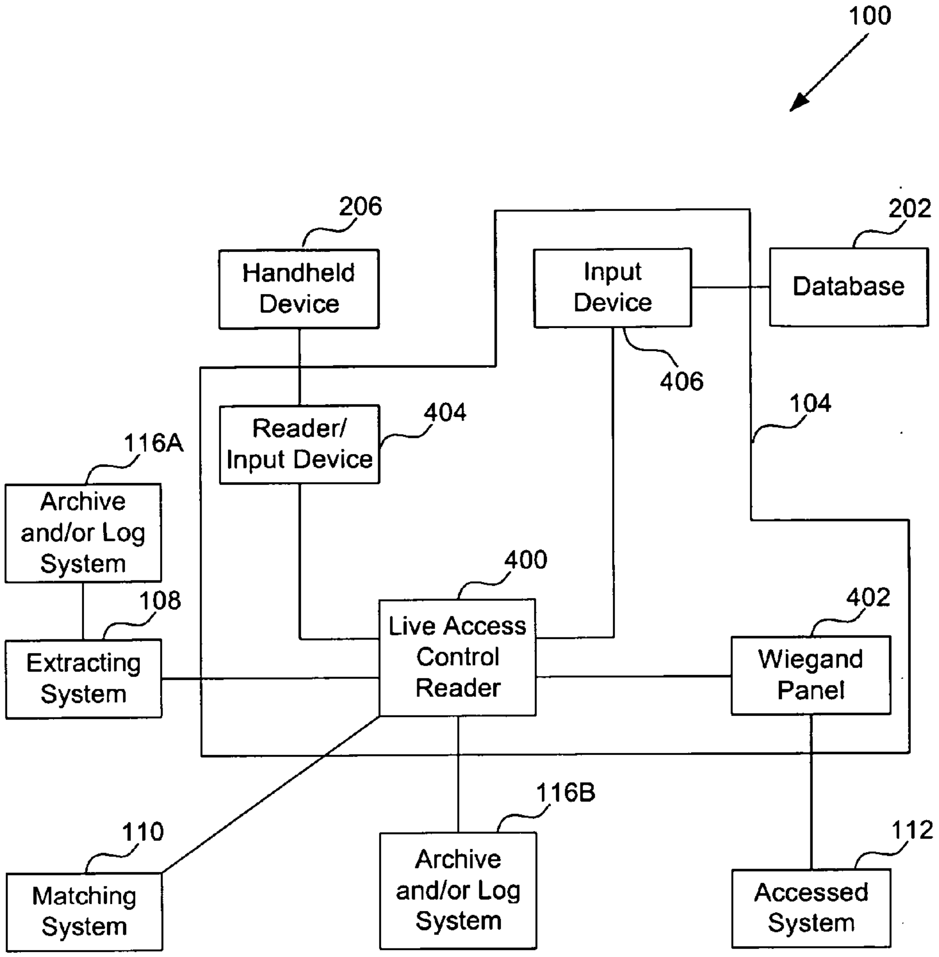

100
206
Handheld Device
Input Device
202
Database
406
404
Reader/ Input Device
104
116A
Archive and/or Log System
400
108
Live Access Control Reader
402
Extracting System
Wiegand Panel
116B
110
112
Matching System
Archive and/or Log System
Accessed System

FIG. 4

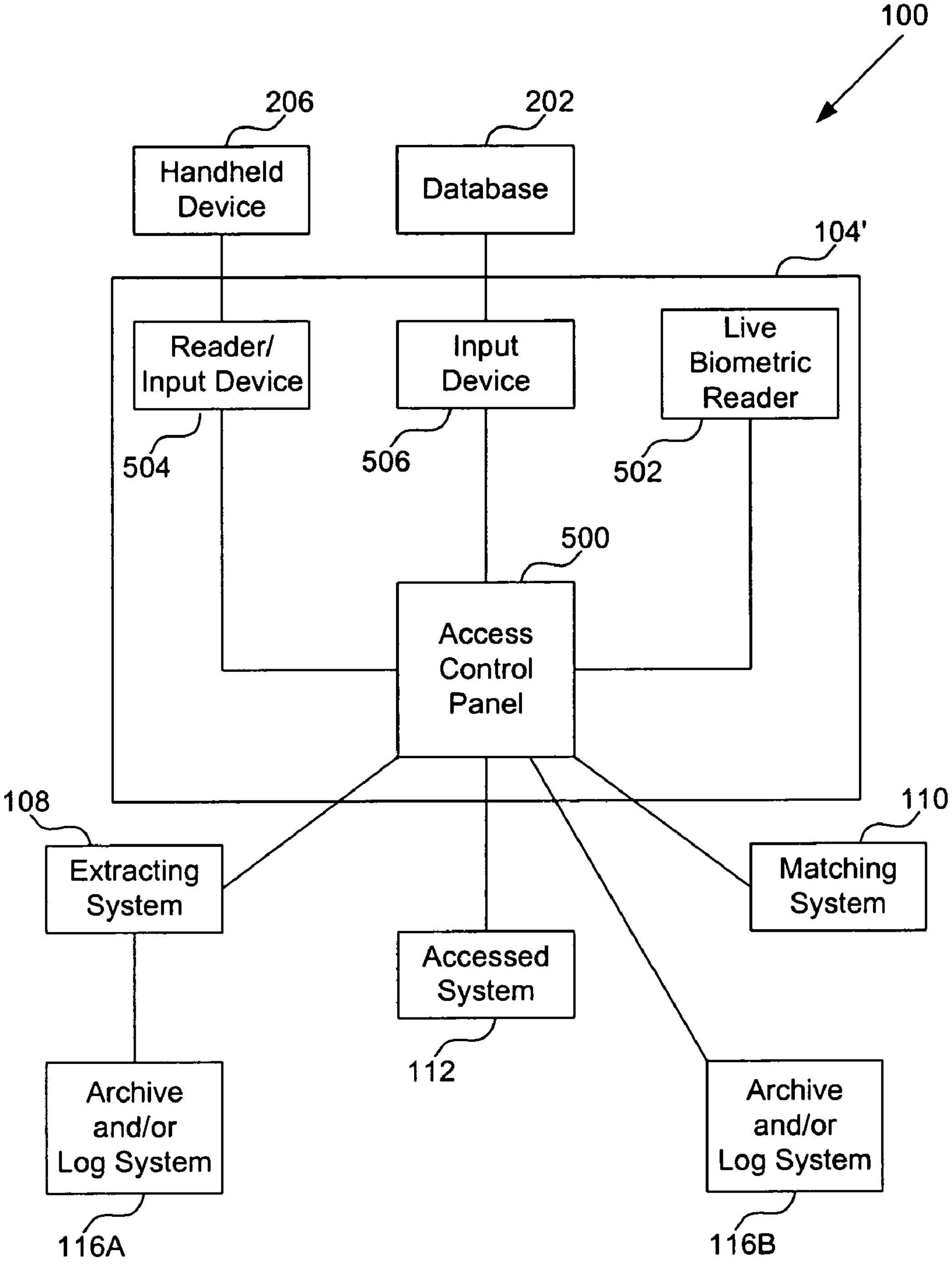
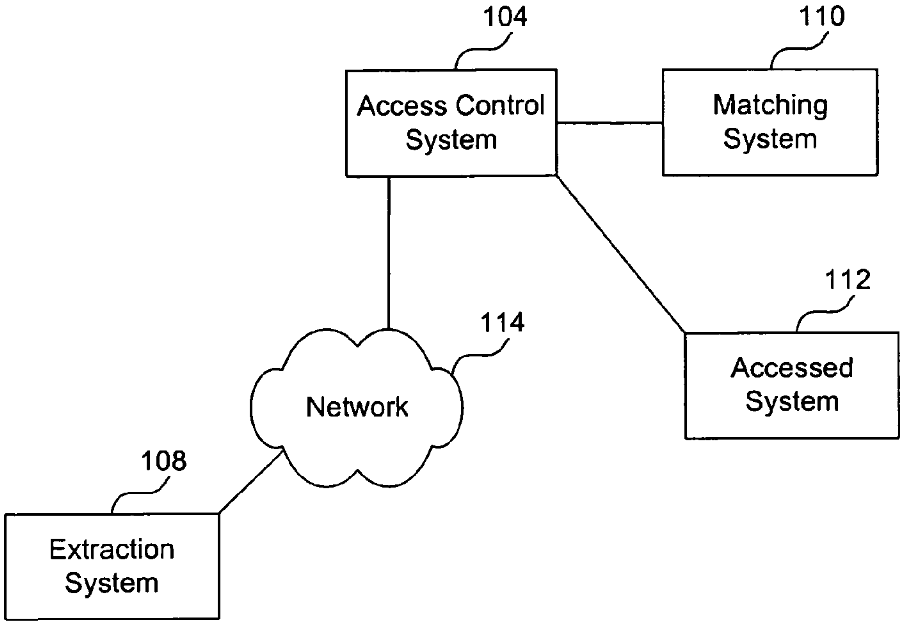

100
206
Handheld Device
202
Database
104'
Reader/ Input Device
Input Device
Live Biometric Reader
504
506
502
500
Access Control Panel
108
Extracting System
110
Matching System
Accessed System
112
Archive and/or Log System
116A
Archive and/or Log System
116B

FIG. 5

FIG. 6


104
Access Control System
110
Matching System
112
Accessed System
114
Network
108
Extraction System

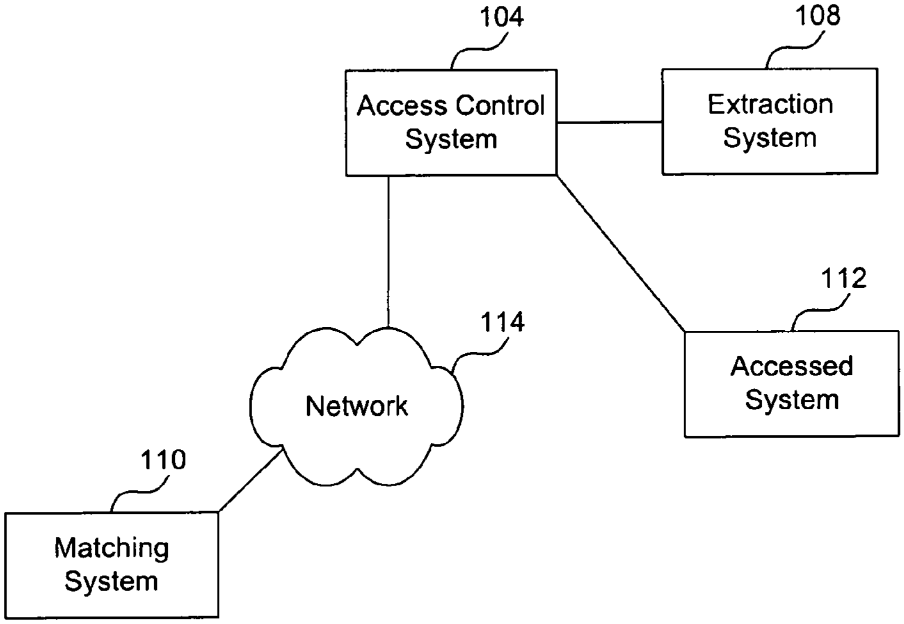

104
Access Control System
108
Extraction System
112
Accessed System
114
Network
110
Matching System

FIG. 7

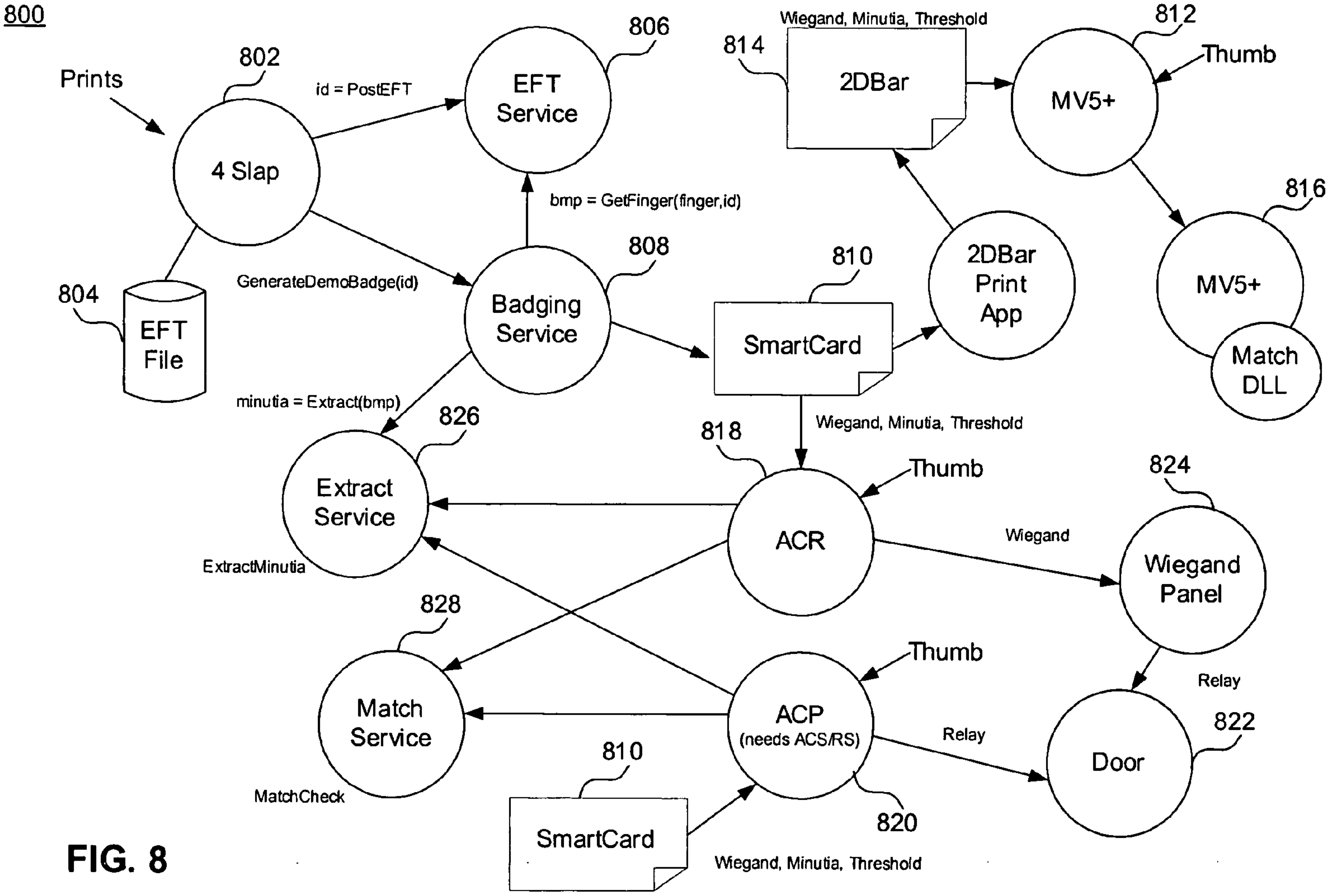

800
Prints
802
4 Slap
804
EFT File
id = PostEFT
806
EFT Service
GenerateDemoBadge(id)
bmp = GetFinger(finger,id)
808
Badging Service
minutia = Extract(bmp)
826
Extract Service
ExtractMinutia
828
Match Service
MatchCheck
810
SmartCard
Wiegand, Minutia, Threshold
814
2DBar
Wiegand, Minutia, Threshold
2DBar Print App
812
MV5+
Thumb
816
MV5+
Match DLL
818
ACR
Thumb
Wiegand
824
Wiegand Panel
Relay
822
Door
ACP
(needs ACS/RS)
Thumb
Relay
820
810
SmartCard
Wiegand, Minutia, Threshold

FIG. 8

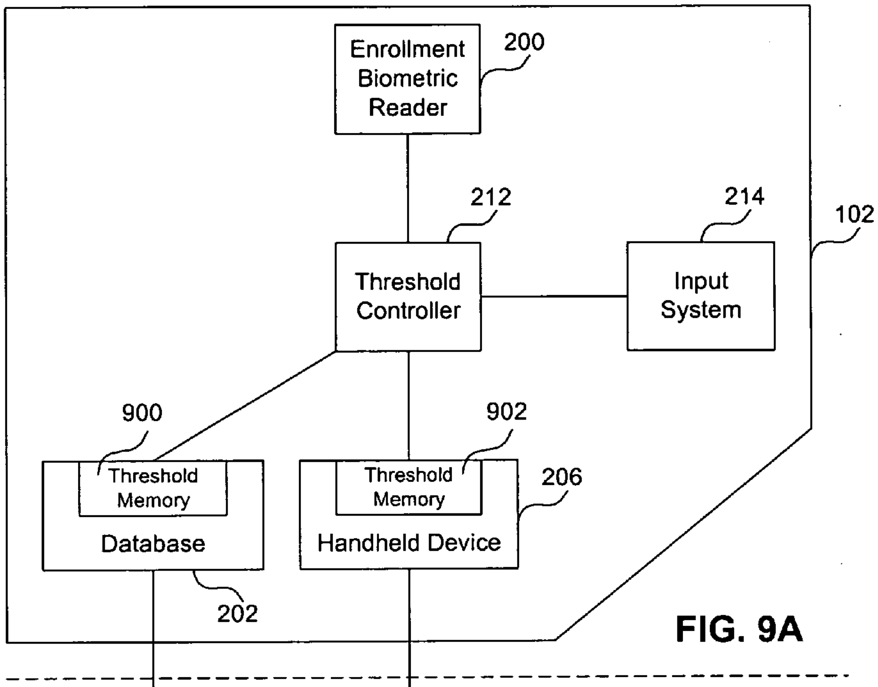

Enrollment Biometric Reader
200
212
214
102
Threshold Controller
Input System
900
902
Threshold Memory
Database
Threshold Memory
Handheld Device
206
202

FIG. 9A

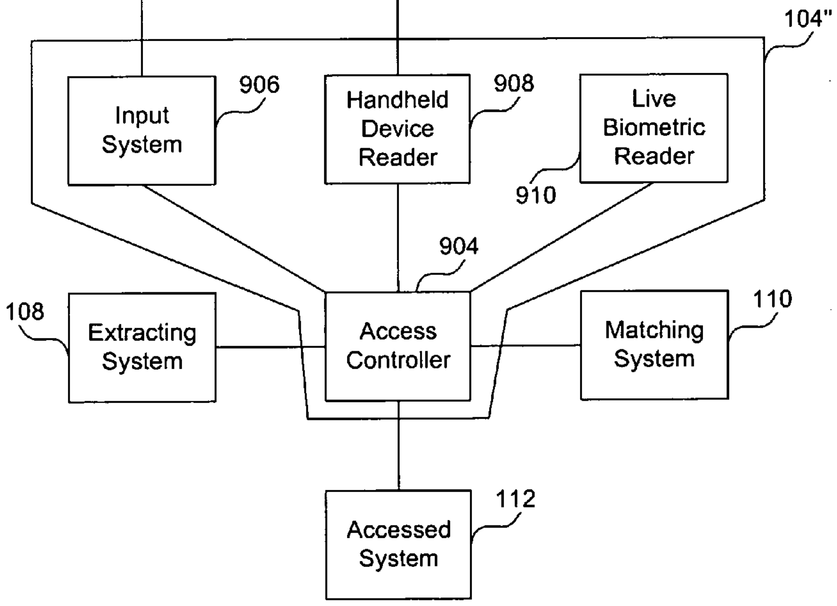

104"
Input System
906
Handheld Device Reader
908
Live Biometric Reader
910
904
108
Extracting System
Access Controller
Matching System
110
Accessed System
112

FIG. 9B

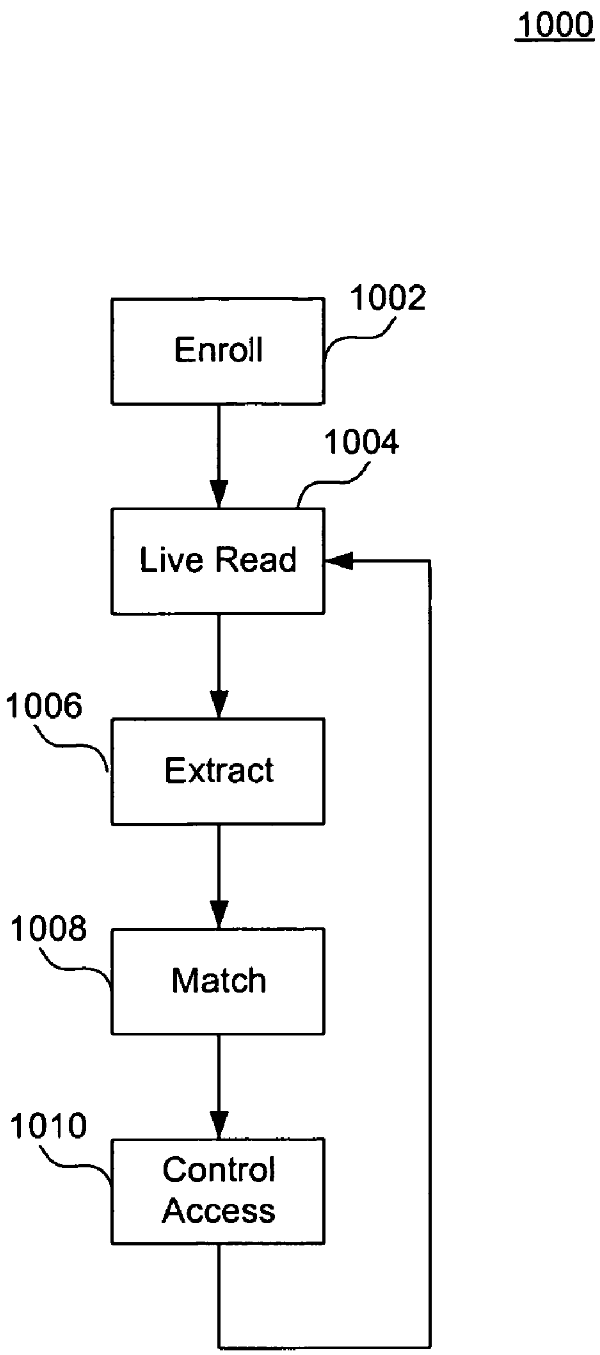

1000
1002
Enroll
1004
Live Read
1006
Extract
1008
Match
1010
Control
Access

FIG. 10

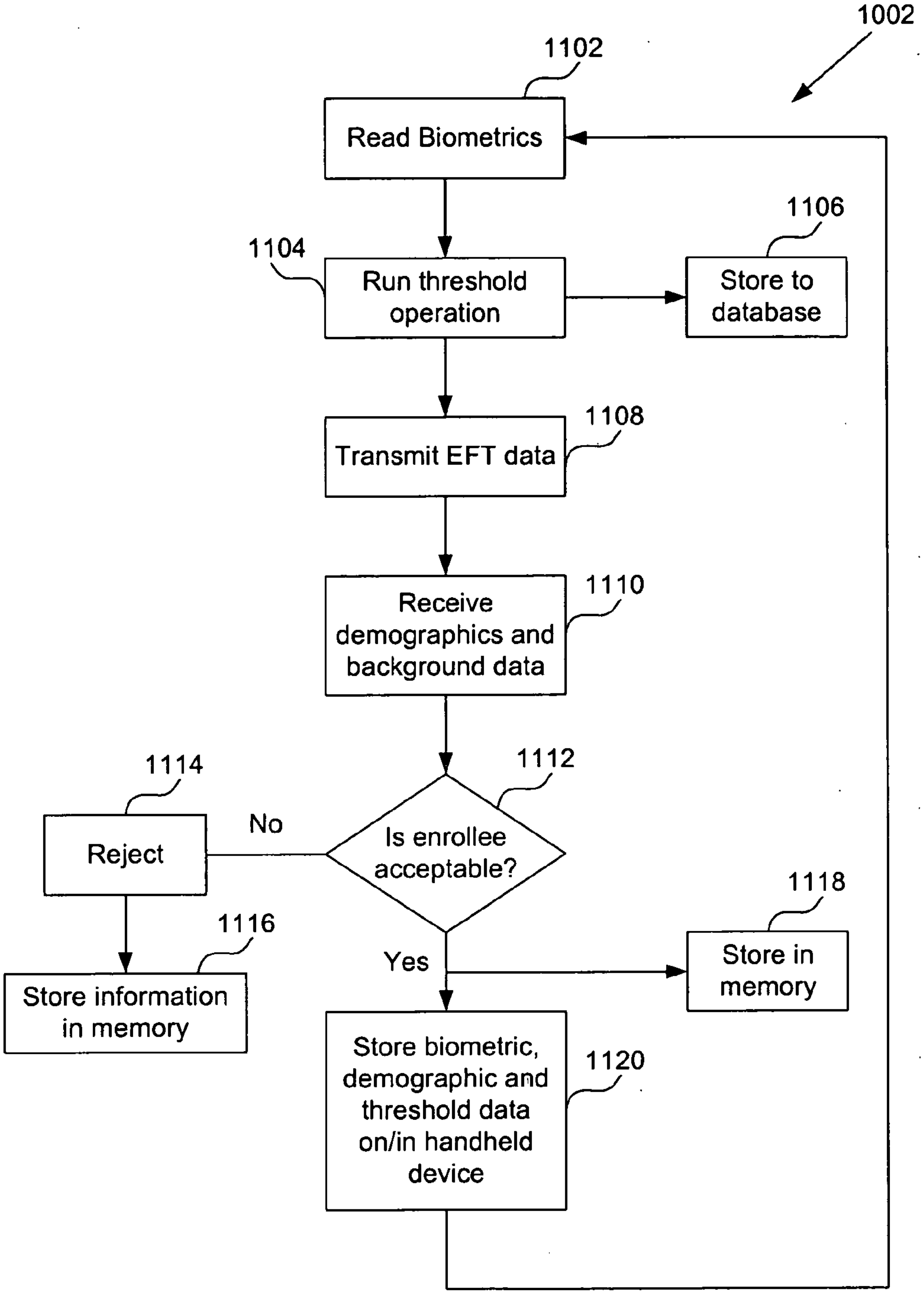

1002
1102
Read Biometrics
1104
Run threshold operation
1106
Store to database
1108
Transmit EFT data
1110
Receive demographics and background data
1112
Is enrollee acceptable?
No
1114
Reject
1116
Store information in memory
Yes
1118
Store in memory
1120
Store biometric, demographic and threshold data on/in handheld device

FIG. 11

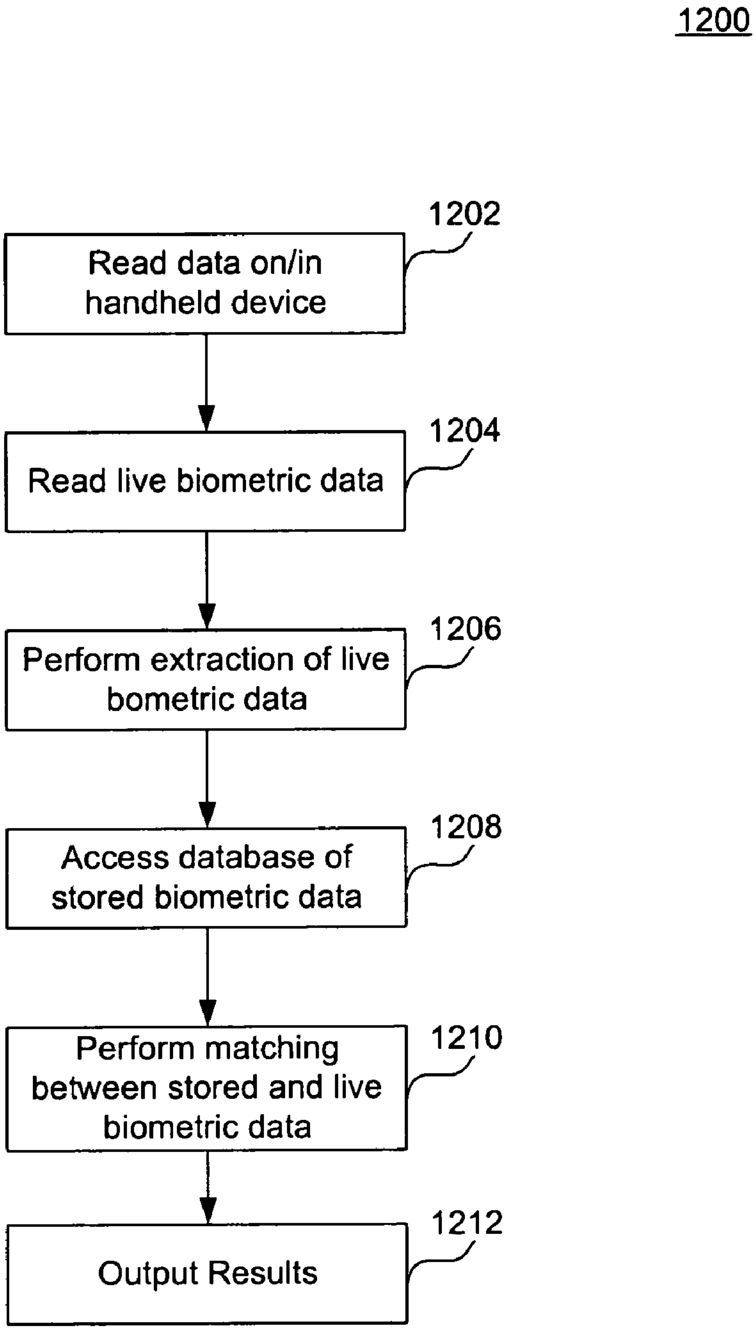

1200
1202
Read data on/in handheld device
1204
Read live biometric data
1206
Perform extraction of live bometric data
1208
Access database of stored biometric data
1210
Perform matching between stored and live biometric data
1212
Output Results

FIG. 12

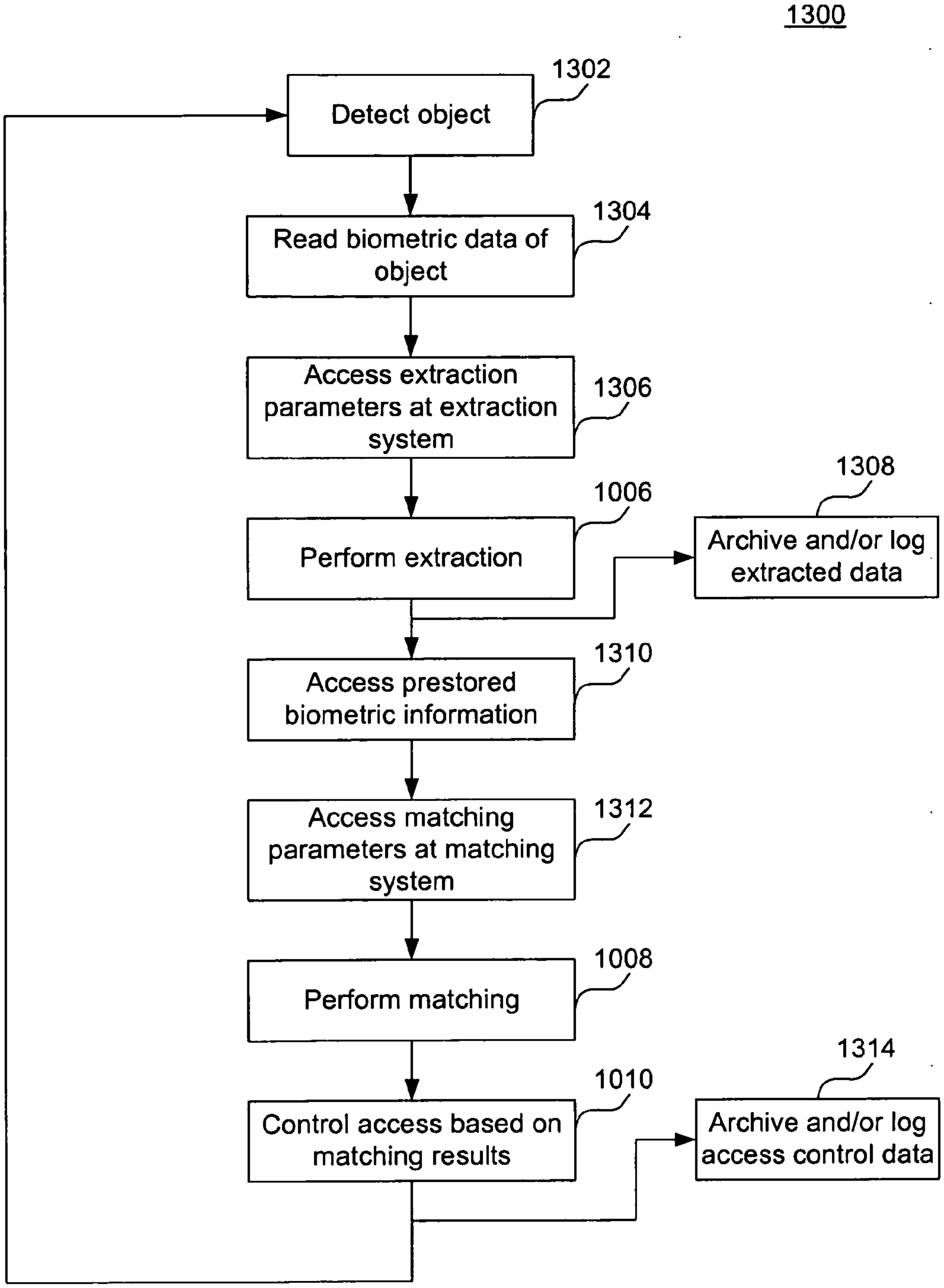

1300
1302
Detect object
1304
Read biometric data of object
1306
Access extraction parameters at extraction system
1006
Perform extraction
1308
Archive and/or log extracted data
1310
Access prestored biometric information
1312
Access matching parameters at matching system
1008
Perform matching
1010
Control access based on matching results
1314
Archive and/or log access control data

FIG. 13

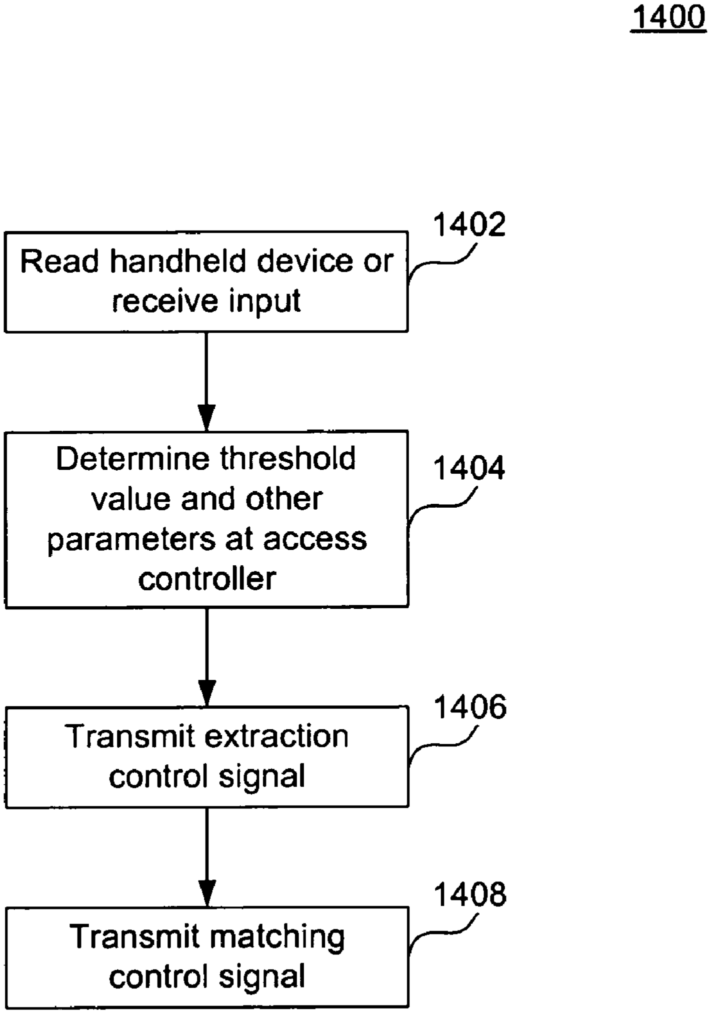

1400
Read handheld device or receive input
1402
Determine threshold value and other parameters at access controller
1404
Transmit extraction control signal
1406
Transmit matching control signal
1408

FIG. 14

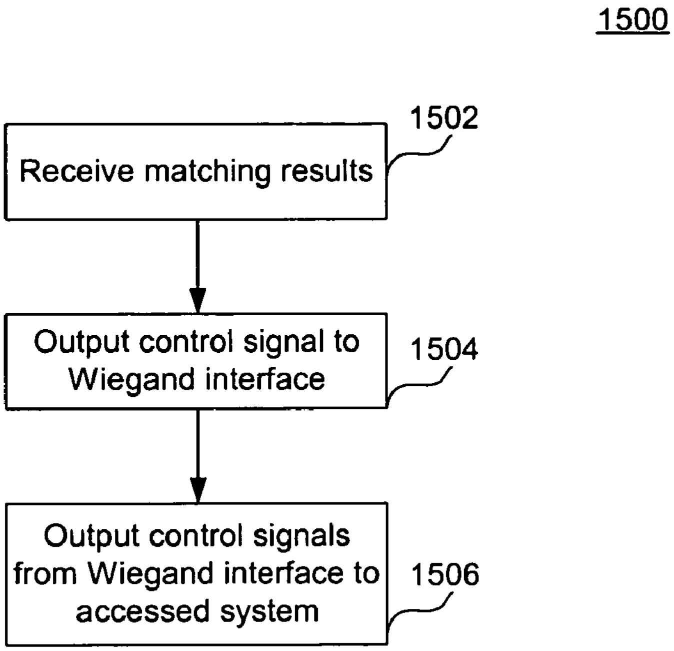

1500
Receive matching results
1502
Output control signal to Wiegand interface
1504
Output control signals from Wiegand interface to accessed system
1506

FIG. 15

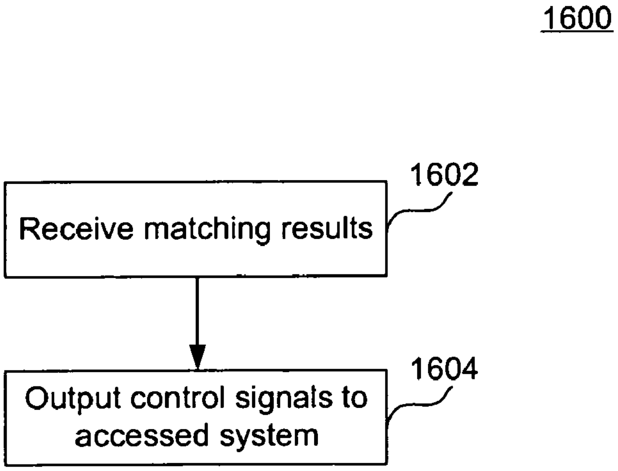

1600
Receive matching results
1602
Output control signals to accessed system
1604

FIG. 16

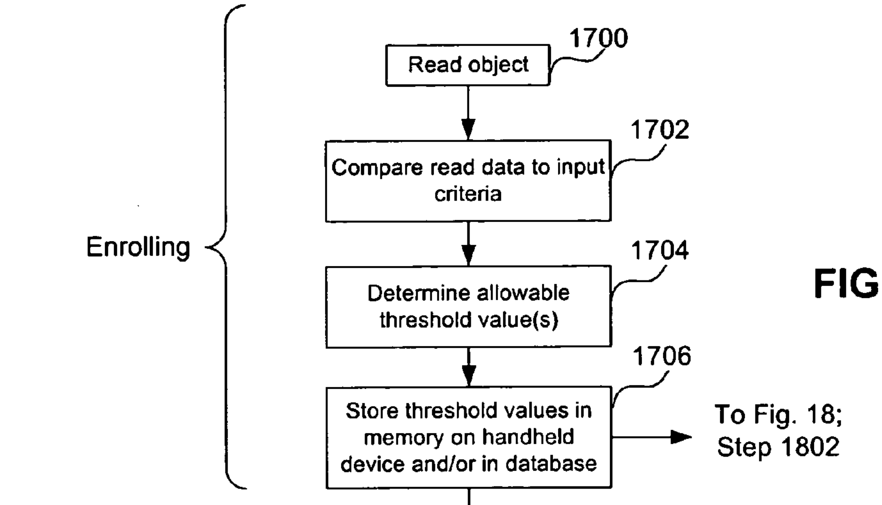

Enrolling
1700
Read object
1702
Compare read data to input criteria
1704
Determine allowable threshold value(s)
1706
Store threshold values in memory on handheld device and/or in database
To Fig. 18; Step 1802

FIG. 17A

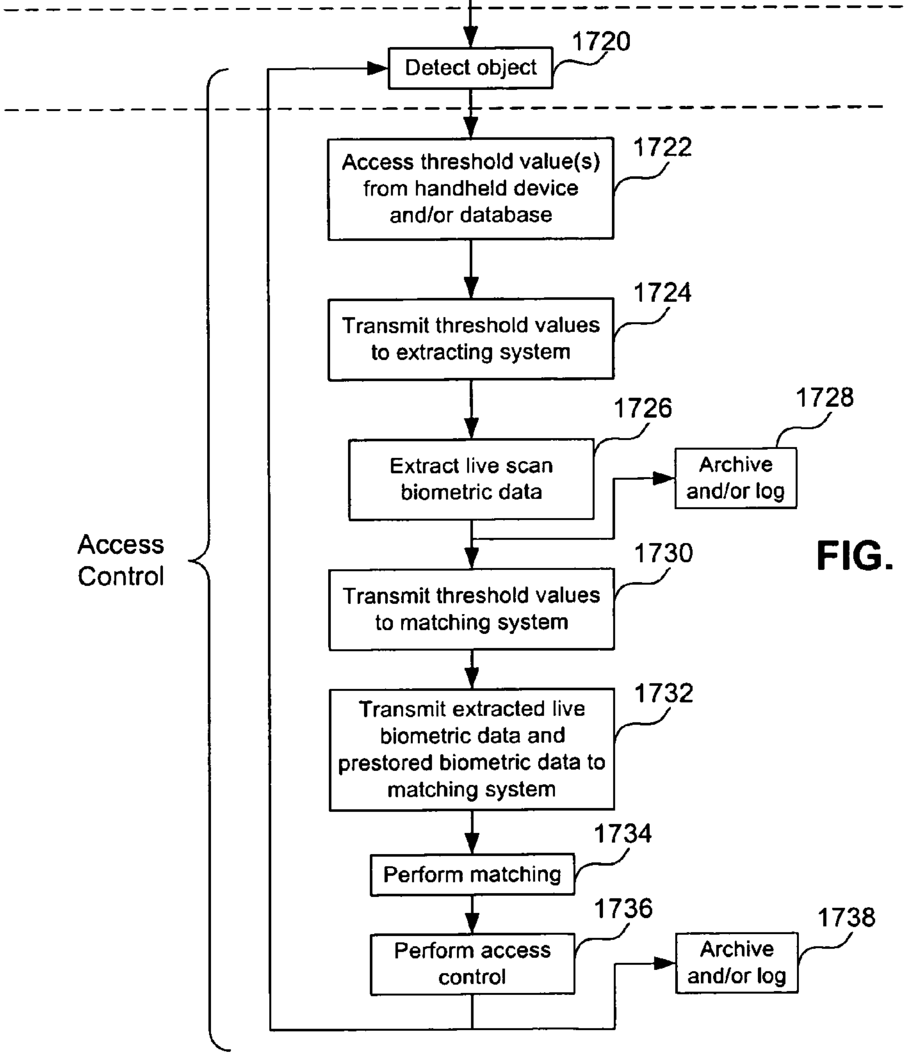

1720
Detect object
Access Control
1722
Access threshold value(s) from handheld device and/or database
1724
Transmit threshold values to extracting system
1726
Extract live scan biometric data
1728
Archive and/or log
1730
Transmit threshold values to matching system
1732
Transmit extracted live biometric data and prestored biometric data to matching system
1734
Perform matching
1736
Perform access control
1738
Archive and/or log

FIG. 17B

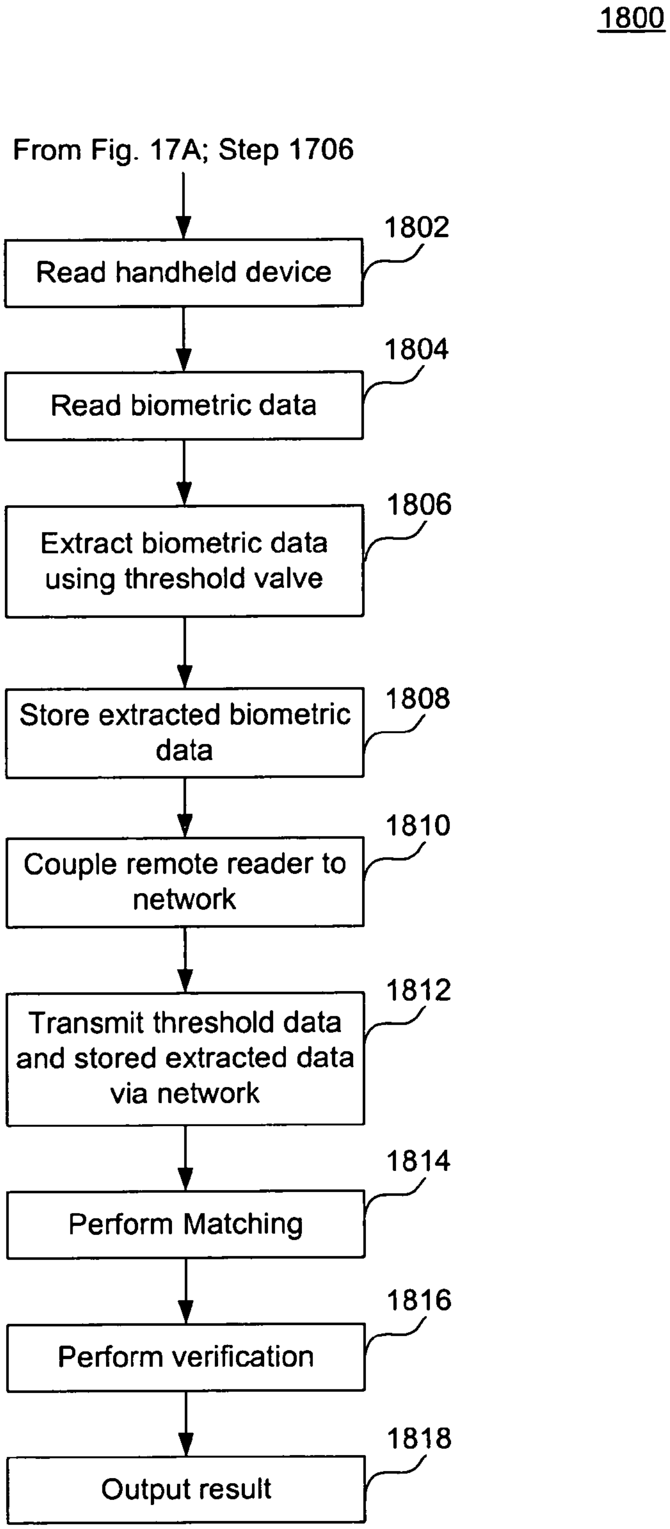

1800
From Fig. 17A; Step 1706
Read handheld device
1802
Read biometric data
1804
Extract biometric data using threshold valve
1806
Store extracted biometric data
1808
Couple remote reader to network
1810
Transmit threshold data and stored extracted data via network
1812
Perform Matching
1814
Perform verification
1816
Output result
1818

FIG. 18

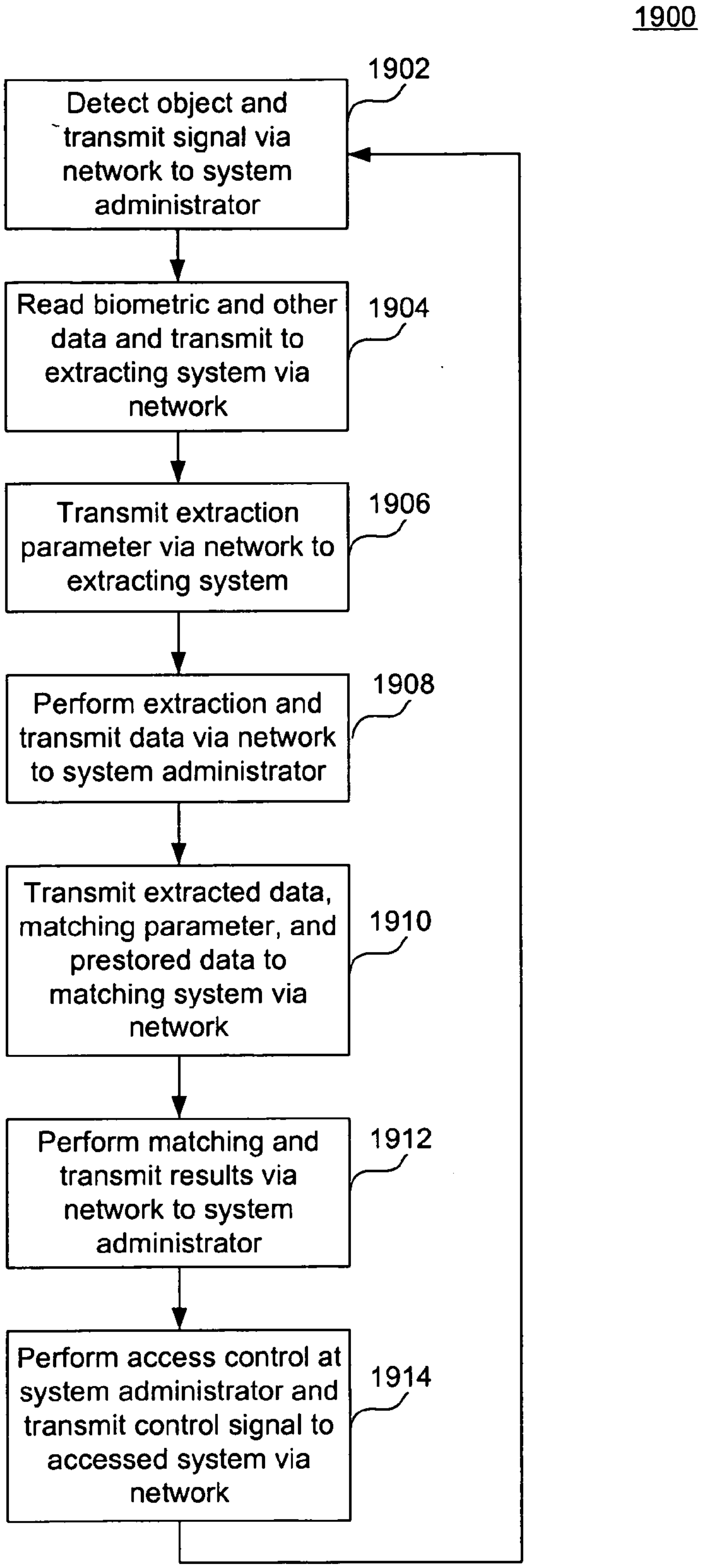

1900
1902
Detect object and transmit signal via network to system administrator
1904
Read biometric and other data and transmit to extracting system via network
1906
Transmit extraction parameter via network to extracting system
1908
Perform extraction and transmit data via network to system administrator
1910
Transmit extracted data, matching parameter, and prestored data to matching system via network
1912
Perform matching and transmit results via network to system administrator
1914
Perform access control at system administrator and transmit control signal to accessed system via network

FIG. 19

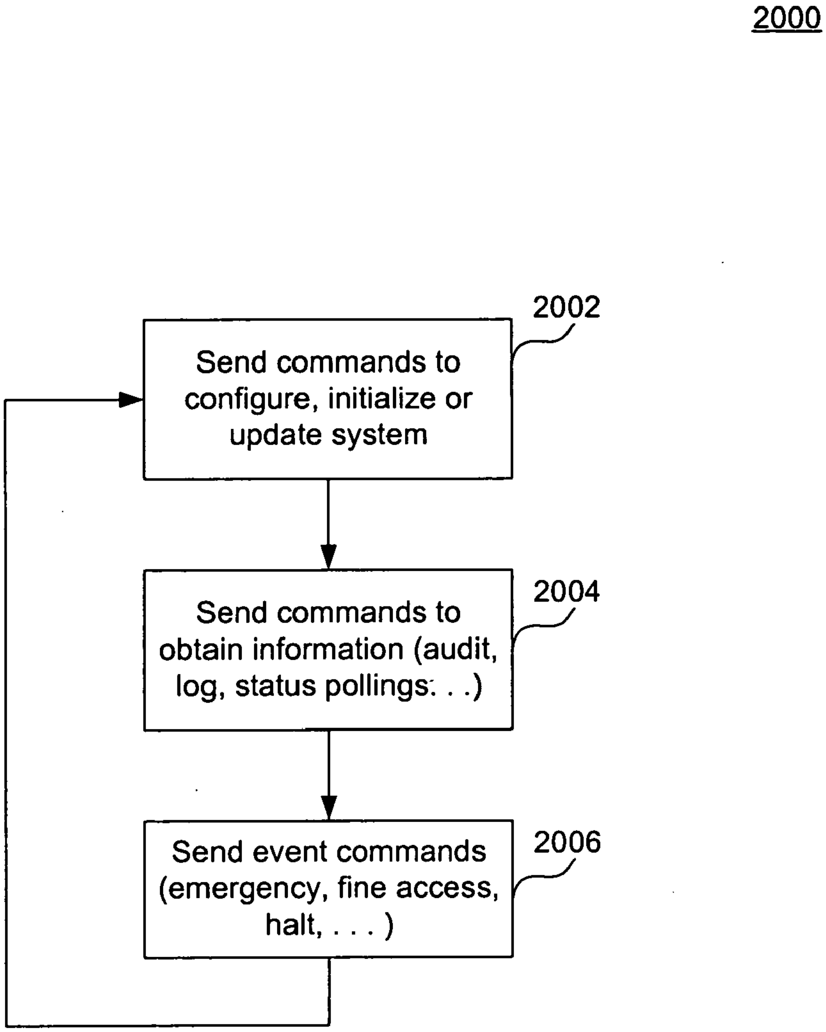

2000
2002
Send commands to configure, initialize or update system
2004
Send commands to obtain information (audit, log, status pollings: . .)
2006
Send event commands (emergency, fine access, halt, . . .)

FIG. 20

SYSTEMS AND METHODS UTILIZING BIOMETRIC DATA

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of U.S. Ser. No. 10/125,650, filed Apr. 19, 2002, which is incorporated herein by reference in its entirety.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention is directed to the field of access control and remote identity verification, in particular, utilizing biometric technology.

[0004] 2. Related Art

[0005] Access control systems are used to limit access to selected individuals. Some of these systems use biometric technologies to determine whether access for an individual will be granted or denied. A biometric is a unique, measurable characteristic or trait of a human being for automatically recognizing or verifying identity. For instance, fingerprint biometrics are largely regarded as an accurate method of biometric identification and verification. See, e.g., Roethenbaugh, G. Ed., *Biometrics Explained* (International Computer Security Association: Carlisle, Pa. 1998), pages 1-34, which is herein incorporated by reference in its entirety. Access control units (ACUs) may be placed locally to perform a biometric analysis on the individual, and determine whether access will be granted or denied. As the number of people needing access to facilities grows, so must be any database holding their biometric information. Eventually, this will become a prohibitive aspect of access control because of the cost, both in equipment and updating time, required to maintain an ever increasing amount of stored biometric data.

[0006] What is needed is a system utilizing a device that stores data for an unlimited number of enrollees allowing easy scalability. Also, a system is needed that utilizes a device that allows for easy updating of stored biometric information to keep all information current for all enrollees.

BRIEF SUMMARY OF THE INVENTION

[0007] Embodiments of the present invention provide a system including an enrollment system that controls storing of biometric data. The system further includes an access control system that reads the stored biometric data, an extracting system coupled to the access control system that extracts live biometric data, and a matching system coupled to the access control system that compares the stored biometric data to the live read biometric data to generate a matching result that is transmitted to the access control system. The system further includes an accessed system coupled to the access control system into which admittance is either allowed or denied based on the matching result. The system may also include a threshold controller that determines and generates a threshold value to be used during extracting, matching, or both. Using the threshold value increases the number of enrollees successfully managed by an access control system, and reduces the number of false rejections of entry. Thresholds can also provide more data with which to make an access control decision rather than mere presentation of a biometric input. These thresholds are individualized and help to make a more informed security decision that, among other things, reduces the rejection of more difficult to read fingerprints.

[0008] Other embodiments of the present invention provide a method including the step of enrolling enrollees and storing their biometric data. The method further includes the steps of performing a live read of one of the enrollees using a reader in an access control system, extracting live biometric data during the live read in an extracting system, and comparing the extracted live biometric data with the stored biometric data in a matching system and outputting a matching result. The method further includes the step of performing access control based on the matching result. The method also includes the steps of determining and generating a threshold value to be used during extracting, matching, or both.

[0009] According to a further feature, processing is distributed across a networked system. In one embodiment, extraction is carried out remotely over a network. In another embodiment, matching is carried out remotely over a network. In this way, an access control reader or panel need not perform extraction and matching, which reduces processing requirements at the access control reader or panel. Processing of extraction and matching is more efficiently managed at the remote sites, for example different extraction or matching algorithms, or changes thereto, can be more easily implemented. Further, the system is more scalable as additional, cheaper access control readers and panels utilizing biometric data can be easily added.

[0010] According to a further feature, in one embodiment the access control system is easily installed as an upgrade to an existing Wiegand panel through the use of a live access control reader, which acts as an interface to a Wiegand panel.

[0011] Some advantages of the system and method may be that they provide an access control system and method that utilizes a device allowing for data to be stored for an unlimited number of enrollees allowing easy scalability. Also, a system and method are provided that utilize a device requiring little, if any, updating time to keep current stored biometric information for all enrollees.

[0012] Further embodiments, features, and advantages of the present inventions, as well as the structure and operation of the various embodiments of the present invention, are described in detail below with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS/FIGURES

[0013] The accompanying drawings, which are incorporated herein and form a part of the specification, illustrate 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 to make and use the invention.

[0014] **FIG. 1** shows an example biometric-based system according to embodiments of the present invention.

[0015] **FIG. 2** shows example elements of an enrolling system in **FIG. 1**.

[0016] **FIG. 3** shows example elements of a remote verification system in **FIG. 1**.

[0017] **FIG. 4** shows example elements of the system of **FIG. 1** with an access control reader in an access control system.

[0018] **FIG. 5** shows example elements of the system of **FIG. 1** with an access control panel in an access control system.

[0019] **FIG. 6** shows example elements of the system of **FIG. 1** with a networked extracting system.

[0020] **FIG. 7** shows example elements of the system of **FIG. 1** with a networked matching system.

[0021] **FIG. 8** shows an example system according to embodiments of the invention.

[0022] **FIG. 9A** shows example elements of the system of **FIG. 1** with a threshold logic system in an enrolling system.

[0023] **FIG. 9B** shows example elements of the system of **FIG. 1** that read the threshold logic value stored in a memory in the system of **FIG. 9A**.

[0024] **FIG. 10** shows example method steps to perform a biometric-based operation according to embodiments of the present invention.

[0025] **FIG. 11** shows example method steps to perform the enroll operation in **FIG. 10**.

[0026] **FIG. 12** shows example method steps to perform a remote verification operation according to embodiments of the present invention.

[0027] **FIG. 13** shows example method steps to perform the access control operation in **FIG. 10**.

[0028] **FIG. 14** shows example method steps to perform the access control operation of **FIG. 10** when a threshold value is used.

[0029] **FIG. 15** shows example method steps to perform an access control operation of **FIG. 10** using an access control reader.

[0030] **FIG. 16** shows example method steps to perform an access control operation of **FIG. 10** using an access control panel.

[0031] **FIG. 17A** shows example method steps to perform a threshold value generation operation during the enrolling operation of **FIG. 10**.

[0032] **FIG. 17B** shows example method steps to use a threshold value generated during the enrolling operation as shown in **FIG. 17A** during an access control step in **FIG. 10**.

[0033] **FIG. 18** shows example method steps to use a threshold value generated during the enrolling operation as shown in **FIG. 17A** during a remote verification operation according to embodiments of the present invention.

[0034] **FIG. 19** shows example method steps to remotely manage access control using a system administrator according to embodiments of the present invention.

[0035] **FIG. 20** shows example method steps to remotely manage access control using a system administrator according to embodiments of the present invention.

[0036] The present invention will now be described with reference to the accompanying drawings. In the drawings, like reference numbers indicate identical or functionally similar elements. Additionally, the left-most digit(s) of a reference number identifies the drawing in which the reference number first appears.

DETAILED DESCRIPTION OF THE INVENTION

[0037] Overview and Terminology

[0038] Some embodiments of the present invention are directed to systems and methods that perform access control and mobile identity verification, including examples utilizing a handheld device, with a memory that stores at least biometric data, such as minutia. The handheld device may also store other data, such as a threshold value and Wiegand data. The data may be stored in a memory, a magnetic strip, a machine-readable code, a bar code, or in all of these devices associated with the handheld device. The handheld device may be a SmartCard or the like.

[0039] One example of biometric data that may need the threshold value is a value indicative of a fingerprint image capture quality of an individual. For example, a low value can indicate a relative poor image capture quality, while a high value can indicate a relative high capture quality. Low threshold values may be appropriate for individuals with difficult to read fingerprints, such as those with dry fingers, missing or damaged fingers, or birth defects. High threshold values may be appropriate for individuals with easy to read fingerprints, such as those with oily fingers or with complete fingertips having a number of distinct minutiae. In some embodiments of the invention, threshold values can be numeric values or categorical values (such as good, average, poor). These threshold values can be used in a variety of ways in the systems of the present invention to accommodate an even greater range of biometric objects successfully managed by the system. The threshold value is used during extracting, matching, or both, to most accurately determine the identity and characteristics of an individual wanting access to an accessed system or being questioned by law enforcement in the field.

[0040] An object as used throughout the specification may be a physical part of an individual, such as an eye, a finger, a limb, etc. An accessed system as used through the specification may be any known system that requires some limitation to entry, which can be a computer, electrical or mechanical equipment, a room, a hallway, a building, a section of a compound, etc. An enrollee as used throughout the specification may be any individual, whether within a business setting, public setting, or otherwise. As mere examples, an enrollee may be an employee of a company, a person receiving governmental assistance, a prisoner, or a person at a traffic stop. Matching used throughout the specification relates to matching either 1:1 to determine if the individual matches with whom he/she says he/she is or 1:m, where m=all the enrollees, to determine if an individual is an enrollee at all.

[0041] Overall Access Control and Remote Verification System

[0042] With reference to **FIG. 1**, a system **100** is shown according to some embodiments of the present invention.

The system **100** may perform access control and remote identity verification. The system **100** includes an enrolling system **102**, an access controller system **104**, a mobile verification system **106**, an extracting system **108**, a matching system **110**, and an accessed system **112**. In some embodiments the systems **102-112** may be coupled together via one or more networks **114**, while in other embodiments the systems **102-112** may be directly coupled to each other. In other embodiments, the system **100** may also include an archive and logging system **116**, which may have multiple archiving and logging devices **116**. The archiving system **116** may store bit maps of biometric information at a certain quality for each enrollee and the logging system **116** may keep track of each enrollee or each accessed system **112**. As mere examples, logging may be used for an audit trail of an enrollee's movements or how many time access is allowed or denied for an accessed system **112**. In still further embodiments, the system **100** may also include a system administrator **118** for remote management of the system **100**.

[0043] Enrolling System

[0044] Now turning to **FIG. 2**, details of the enrolling system **102** according to embodiments of the present invention are shown. The enrolling system includes a biometric reader **200** coupled to a database **202**, where the read biometric information is stored in a memory of the database **202**. In other embodiments, either in addition to or in place of the database **202**, the biometric reader can be coupled to a handheld device controller **204** that is coupled to a handheld device **206**. In these embodiments, the read biometric data is stored in a memory in or on the handheld device **206**. In some embodiments, the handheld device **206** may be a SmartCard or the like.

[0045] Through use of this handheld device **206** the need for a large database is virtually eliminated because biometric and other personal data can be stored on the handheld device **206**. There would also be no need to update a central database, just the hand held device **206** memory, which ensures more accurate information is timely maintained. The use of the handheld device **206** is most effective for systems that have a large and continuously growing enrollee list.

[0046] In embodiments where the biometric reader **200** reads and extracts fingerprints, the biometric reader **200** may be coupled between an electronic fingerprint template (EFT) file **208** and an EFT service **210**. The EFT file **208** converts read fingerprint data into a predetermined form and transmits the data to the EFT Service **210**, which may be the Federal Bureau of Investigations (FBI), other federal, state, or local authorities, private entities, or the like. This data is then used by the EFT Service **210** to run background checks on possible enrollees.

[0047] In still other embodiments the enrolling system **102** may include a threshold controller **212** coupled between the biometric reader **200**, the handheld device controller **204** and/or the database **202**, and an input system **214**. According to one feature, threshold values associated with each biometric input are assigned and stored during enrollment in an enrolling system. In this way, the assignment and storage of correct or suitable thresholds can be obtained during enrollment. This may have advantages in many practical situations where more experienced personnel are available at enrollment to monitor threshold value assignment and storage. Also, the presentation of biometric input at enrollment may often occur in a setting where more time is available for ensuring proper threshold values are assigned and quality biometric data, such as fingerprint data, are captured. Details of the threshold controller **212** are described below with reference to **FIG. 9A-9B** and **FIGS. 17A-17B**.

[0048] Mobile Verification System

[0049] Now turning to **FIG. 3**, details of the mobile verification system **106** according to embodiments of the present invention are shown. The mobile verification system **103** includes a reading device **300** coupled to a verification system **302**. In some embodiments the reading device **300** only includes a live biometric reader **304**. In other embodiments the reading device **300** also includes a code reader **306**. This system may be utilized by law enforcement officials in the field to determine the identity of individuals. The handheld device **206** may include a machine-readable code or a one dimensional or two-dimensional bar code (not shown for convenience) as is known in the art. This code may contain biometric data, a threshold value, or other information that can be used in determining the identity of individuals. The handheld device **206** may also include a magnetic stripe, or the like, that can be read by the verification system **302** to gain additional information. An example of other information or data may be an electronic "signature" by a trusted source that authenticates the handheld device **206**. Thus, in this environment, the handheld device **206** may be a driver's license, SmartCard, or the like. In one example, the verification system **302** may be a law enforcement field computer (not shown) with a USB port that couples the reader **300** via the network **114** to a central processing system.

[0050] According to one embodiment, the reader **300** is a handheld, mobile device. This is helpful in allowing capture of biometric data at different locations. Individuals can be checked during spot checks, mobile or roving checks, and in other ways to provide additional security in support of access control systems. This is especially helpful in applications such as airport security, where spot checks need to be performed on a tarmac or runway, in a terminal, etc. Other applications that require mobile verifications also benefit from the mobile reader **300**. Wireless links can also be used to transfer data from the mobile reader **300** to the verification system **302**.

[0051] Access Control Apparatus

[0052] Access Control Reader

[0053] **FIG. 4** shows details of the access control system **104** in the system **100** according to embodiments of the present invention. The access control system **104** includes a live access control reader **400** and a Wiegand panel **402**. In some embodiments the live access control reader **400** is coupled to a reader/input device **404** that reads the handheld device **206**. In other embodiments the access control reader **400** is coupled to an input device **406**, which may be a key system that accesses information in the database **202** based on correlating entered characters or other input from the input device **406** with stored information in the database **202**. In still other embodiments, the access control reader **400** may be coupled to both the reader **404** and the input device **406**.

[0054] In this arrangement, the live access control reader **400** both reads live biometric data and accesses stored biometric data to be used during an access control operation described in more detail below. Also, in some embodiments an additional level of security can be provided because multiple factors (a live biometric and an input) may be used in access control. This architecture provides significant installation advantages for incorporating aspects of the system **100** into existing stand-alone access control systems having Wiegand panels. For instance, one or more live access control readers **400** can be coupled to one or more existing Wiegand panels **402**. This allows existing stand-alone Wiegand access control systems to be easily upgraded to a more secure, scalable, network-based access control system **100** of the present invention.

[0055] As also seen in **FIG. 4**, the extracting system **108** may be coupled to the archive and/or log system **116**A. Also, the live access control reader **400** may be coupled to the archive and/or log system **116**B.

[0056] Access Control Panel

[0057] Turning now to **FIG. 5**, the access control apparatus **104**' in the system **100** according to embodiments of the present invention is shown. The access control apparatus **104**' includes an access control panel **500** coupled to a live biometric reader **502**. In some embodiments, the access control panel **500** is coupled to a reader/input device **504** that reads the handheld device **206**. In other embodiments, the access control panel **500** is coupled to an input device **506**, which may be a key system that accesses information in the database **202** based on correlating entered characters or other input from the input device **506** with stored information in the database **202**. In still other embodiments, the access control panel **500** may be coupled to both the reader **504** and the input device **506**.

[0058] In this arrangement, the access control panel **500** reads live biometric data and accesses stored biometric data to be used during an access control operation described in more detail below. As described with respect to **FIG. 4**, in some embodiments the use of multiple factors (live biometric data and stored or input data) provides an additional level of security. As also seen in **FIG. 5**, the extracting system **108** may be coupled to the archive and/or log system **116**A. Also, the access control panel **500** may be coupled to the archive and/or log system **116**B.

[0059] Network Extraction or Matching Systems

[0060] As shown in **FIG. 1**, according to a further feature of the present invention, extraction processing can be carried out by a remote extracting system **108** (**FIG. 6**). In this way, processing work is distributed across the system **100**. Hence, the access control system **104**, the access control reader **400**, and the access control panel **500** need not carry out extraction. This reduces the processing requirement at the access control reader **400** or panel **500**. Further, because extraction is handled at a remote site accessed over the network **114**, the system **100** can more easily scale to accommodate more access control readers **400** and/or panels **500** and more enrollees. Different types of extraction, changes in extraction algorithms, or moving processing power to support extraction need only be provided in the extracting system **108** rather than the individual access control readers **400** or the individual access control panels **500**.

[0061] Similar advantages are provided in a feature where matching processing is carried out by a remote matching system **110** (**FIG. 7**). In this way, processing work is distributed across the system **100**. Hence, the access control system **104**, access control reader **400**, and access control panel **500** need not carry out matching. This reduces the processing requirement at the access control reader **400** or panel **500**. Further, because matching is handled at a remote site accessed over the network **114**, the system **100** can more easily scale to accommodate more access control readers **400** and/or panels **500** and more enrollees. Different types of matching, changes in matching algorithms, or moving processing power to support matching need only be provided in the matching system **110** rather than individual access control readers **400** or individual access control panels **500**.

[0062] As seen in **FIGS. 6 and 7**, in some embodiments only the extracting system **108** (**FIG. 6**) or the matching system **110** (**FIG. 7**) may be directly coupled to the rest of the elements **104**, **108**/**110**, and **112** of the system **100**. Thus, either one or both of the extracting system **108** or the matching system **110** would be coupled to the rest of the elements **104**, **108**/**110**, and **112** via the network **114**. The network **114** may be an Intranet, and Internet, or any other type of network or combination of networks known in the art.

[0063] Example Access Control and Remote Verification System

[0064] Shown in **FIG. 8** is an example system **800** that includes features from various embodiments of the present invention, which may be described above or below. In this example, an enrolling system includes a biometric reader **802**, which can be any live biometric scanner manufactured by Cross Match Technologies, Inc., or any other manufacturer. The biometric reader **802** is coupled between the EFT file **804**, which converts read fingerprint data into useable data to be submitted to the EFT Service **806**. The EFT Service **806** provides any information it may have on the individual being enrolled. The information is provided to the Badging Service **808** in order to store the information on a SmartCard **810**. The stored data may be a Wiegand value, a threshold value, and a minutia value.

[0065] In this example, one embodiment of reading the SmartCard **801** may be to use a remote verification system including a mobile reader **812** that reads both a code **814** on the SmartCard **810** and a live fingerprint of an individual to perform matching in the verification system **816**. The reader **812** may be manufactured by Cross Match Technologies, Inc. and the verification system may be a computer either linked or unlinked to a network, such as one found in a law enforcement vehicle.

[0066] Other embodiments used to read and utilize information on the SmartCard **810** are an access control reader (ACR) **818** environment and an access control panel (ACP) **820** environment. Either of these access control systems can be used to control access to a door **822**, either via a Wiegand panel **824** or directly. As shown, both the ACR **818** and the ACP **820** can access the SmartCard **810** to send extracting parameters to an extracting service **826**. Also, both the ACR **818** and ACP **820** can access the SmartCard to send stored biometric data and matching parameters, along with the live read biometric data read by a live biometric reader (not shown), to a matching service **828**. In some embodiments, based on a result from the matching service **828**, the ACR **818** sends Wiegand signal to the Wiegand panel **824** to control opening of the door **822** via a relay signal from the Wiegand panel **824**. In other embodiments, based on a result from the matching service **828**, the ACP **820** sends a relay signal to the door **822** to control its opening.

[**0067**] Threshold Value System

[**0068**] Referencing **FIGS. 9A and 9B**, a portion of the system **100** that determines, generates, stores, and accesses a threshold value utilized in several embodiments of the present invention is shown. A detailed operation will be explained below with reference to **FIGS. 17A, 17B**, and **18**. In the embodiment shown in **FIGS. 9A-9B**, the threshold controller **212** determines a threshold value based on criteria received or accessed from the input system **214** and the biometric data read by the enrollment biometric reader **200**. Basically, the threshold value indicates required levels or tolerances for matching and extracting based on the quality of the read biometric data. The threshold controller **212** then generates a threshold value that is stored in a threshold memory **900** in the database **202**, a threshold memory **902** in the handheld device **206**, or both. Then, when an individual wants to access an accessed system **112**, an access controller **904** accesses the threshold value in the database **202** via input system **906** or accesses the threshold value in the handheld device **206** via the handheld device reader **908**. Either preceding or subsequent to this, the access controller **904** initiates reading of live biometric data of the individual via the live biometric reader **910**. The threshold value is then used by the access controller **904** to further control extracting by the extracting system **108**, matching by the matching system **110**, or both.

[**0069**] As discussed above, one example of biometric data that may need the threshold value is a value indicative of a fingerprint image capture quality of an individual. For example, a low value can indicate a relative poor image capture quality, while a high value can indicate a relative high capture quality. Low threshold values may be appropriate for individuals with difficult to read fingerprints, such as those with dry fingers, missing or damaged fingers, or birth defects. High threshold values may be appropriate for individuals with easy to read fingerprints, such as those with oily fingers or with complete fingertips having a number of distinct minutiae. In embodiments of the invention, threshold values can be numeric values or categorical values (such as good, average, poor). These threshold values can be used in a variety of ways in the system **100** to accommodate an even greater range of biometric objects successfully managed by the system **100**. A threshold value may be a required value or parameter generated from input criteria based on biometric data read and extracted by an extracting system **108** during an enrolling process. The threshold value is used during extracting, matching, or both, to most accurately determine the identity and characteristics of an individual wanting access to an accessed system **112** or being questioned by law enforcement in the field.

[**0070**] Overall Operation

[**0071**] An overall operation **1000** of the system **100** is shown in **FIG. 10**. In step **1002** an individual enrolls in the enrolling system **102** by having their biometric and other data read, extracted, accessed, and stored. A live read of biometric data is taken of an individual in step **1004** when they wish to access an accessed system **112**. The live read biometric data is extracted by the extracting system **108** at step **1008**. A matching operation is performed by the matching system **110** at step **1008** to compare at least the stored biometric data and the live read biometric data. Based on an output from the matching system **110** generated at step **1008**, access to an accessed system **112** is controlled by the access control system **104** at step **1010**.

[**0072**] Enrolling Operation

[**0073**] The details of the enrolling operation **1002** performed by the enrolling system **108** according to embodiments of the present invention are shown in **FIG. 11**. The biometric reader **200** at step **1102** reads an individual's biometric data. In some embodiments, a threshold operation is performed at step **1104** by a threshold controller **212** and a threshold value is stored at step **1106**. In other embodiments, the enrolling operation **1002** moves from step **1102** to step **1108**, during which EFT data generated by the EFT file **208**, which is based on the read biometric data, is transmitted to an EFT service **210**. Information is received from the EFT service **210** at step **1110**. Based on this information, a determination is made whether an enrollee is acceptable at step **1112**. If no, the enrollee is rejected at step **1114**, and their information is stored in a memory in the database **202** at step **1116**. If yes, their biometric and other information is stored in a memory of a database **202** at step **1118**, in a memory of a handheld device **206** at step **1120**, or both. Following this, the enrolling operation **1002** returns to step **1102** and waits for more enrollees.

[**0074**] Remote Verification Operation

[**0075**] A mobile verification operation **1200** performed by the mobile verification system **106** is shown in **FIG. 12**. A law enforcement official in the field would perform this operation most likely during questioning of individuals for a routine traffic stop or during a crime investigation. The remote reader **300** reads data in or on the handheld device **206** during step **1202**. As described above, the handheld device **206** may contain machine-readable code or bar code information that is read by the reader **300**. Live biometric data is read by the reader **300** at step **1204**, which is extracted at step **1206**. The reader **300** is then coupled to a database at step **1208**, which may be through use of either a wireless or wired system. For example, the reader **300** may have a USB jack and a law enforcement computer (not shown) may have a USB port. By coupling the reader **300** to the database, the read handheld device data and the live biometric data can be compared or matched with database information at step **1210**. Based on this comparison or matching, the law enforcement official in the field can receive timely output as to information on the individual at step **1212**. Thus, through the use of the handheld device **206** storing data, a more accurate and timely assessment of the situation can be made in the field.

[**0076**] This roving or mobile verification operation **1200** can be used to supplement the security provided by the system **100**.

[**0077**] Access Control Operation

[**0078**] Extracting, Matching, and Controlling Operations

[**0079**] Referencing **FIGS. 13-14**, several aspects of the overall access control operation **1000** are shown. In some embodiments that have stand-by modes to save power consumption, or other similar functions, an object is detected at an accessed system **112** at step **1302**. In other embodiments where there is no special mode, step **1302** may be optional. The biometric data of the object is read at step **1304** by live access control reader **400**, the live biometric reader **502**, or the live biometric reader **910**, or any other reader. The extracting system **108** accesses extraction parameters from the access control system **104** at step **1306**. The extraction parameters may be related to a required image quality, contrast ratio, whether the image is white-on-black or black-on-white, whether the image can be or should be cropped, how many minutiae must be extracted, or the like. The extracting step **1006** is then performed. In some embodiments, extracted data is archived and/or logged in the archiving and logging system **116** at step **1308**. In other embodiments, stored biometric data is accessed by the matching system **110** at step **1310** without performing step **1308**. The matching system **110** accesses matching parameters at step **1312**. Matching is performed at step **1008** by comparing the live read biometric data to the stored biometric data. Access is controlled at step **1010** based on results from the matching step **1008**. In some embodiments, the matching results or other control data received at the access controller **104** are archived and/or logged in the archiving and logging system **116** at step **1314**. In other embodiments, the operation **1300** returns to step **1302** to await detection of another object.

[**0080**] The extraction parameter step **1306** and the matching parameter step **1312** are performed along with an operation **1400** shown in **FIG. 14**. Some of the parameters are determined by reading the handheld device **206** or receiving information from the input device **406**, **506**, or **906** at step **1402**. Depending on the embodiment, values for threshold and other parameters are determined by the access control system **104** at step **1404**. After receiving the request for extraction parameters at step **1306**, the extraction parameters are transmitted at step **1406**. Also, after receiving the requests for matching parameters at step **1312**, the matching parameters are transmitted at step **1408**.

[**0081**] Access Control Reader Operation

[**0082**] After performing the operations shown in **FIGS. 13-14**, the access control system **104** of **FIG. 4** performs an access control operation **1500**, which is shown in **FIG. 15**. The live access control reader **400** receives matching results from the matching system **110** at step **1502**. Based on the results, the live access control reader **400** outputs a control signal to a Wiegand panel **402** at step **1504**. In turn, the Wiegand panel **402** sends a relay or control signal to the accessed system **112** at step **1506**.

[**0083**] Access Control Panel Operation

[**0084**] Similar to the operation shown in **FIG. 15**, after performing the operations shown in **FIGS. 13-14**, the access control system **104'** of **FIG. 5** performs an access control operation **1600**, which is shown in **FIG. 16**. Due to the fact the system in **FIG. 5** has a central access control panel **500**, and not just an access control reader **400**, more direct control of the accessed system **112** can be achieved. Thus, matching results from the matching system **110** are received at the access control panel **500** at step **1602**. Based on the results, the access control panel **500** sends a control or relay signal directly to the accessed signal **112** at step **1604**.

[**0085**] Threshold Value Operation

[**0086**] A threshold value determination and generation operation **1104**, and how the generated threshold value is utilized, are shown in more detail in **FIGS. 17A, 17B**, and **18**. The biometric reader **200** at step **1700** reads biometric data of an object. The read biometric data is processed by the threshold controller **212** by comparing the quality or other aspects of the data with criteria input via the input system **214** at step **1702**. Based on this comparison, a threshold value(s) is determined for each type of biometric data at step **1704**. For example, as discussed above, a low quality print would result in one threshold value, while a high quality print would result in another threshold value. The threshold value is stored either in the memory **900** of the database **202**, the memory **902** of the handheld device **206**, or both at step **1706**. If the access control operation **1300-1400** is performed with the threshold value, the use of the threshold value is shown in **FIG. 17B**. Otherwise, if the mobile verification operation **1200** is performed with the threshold value, the use of the threshold value is shown in operation **1800** in **FIG. 18**.

[**0087**] As seen in **FIG. 17B**, an object is detected at step **1720**. The threshold value is accessed by an access controller **400, 500**, or **904** at step **1722** from either memory **900** or memory **902**. The threshold value is transmitted to the extracting system **108** at step **1724**. The threshold value is used during an extraction of live biometric information at step **1726**. In some embodiments, the extracted biometric information is archived and/or logged by the archiving and logging system **116** at step **1728**. In other embodiments, the method moves from step **1726** directly to step **1730** and transmits the threshold value to the matching system **110**. The live extracted and stored biometric data are transmitted to the matching system at step **1732**. A matching result is determined in the matching system based on a comparison between the live biometric data and the stored biometric data at step **1734**. A score is generated based on a comparison between the matching result and the threshold value, and the score is used at step **1736** to perform access control by the access controller **400, 500**, or **904**. In some embodiments, information used for access control is archived and/or logged by the archiving and logging system **116** at step **1738**. In other embodiments, the method moves directly from step **1736** back to step **1720** and waits until another object is detected.

[**0088**] As seen in **FIG. 18**, a remote verification operation using threshold data **1800** starts by reading the handheld device **206** with the reader **300** at step **1802**. The reading may include one or all of reading a machine-readable code or a bar code, which may be one or two-dimensional bar code, reading of a magnetic strip, and reading of a memory **902** to access the threshold value, stored biometric data, and other data. The reader **300** at step **1804** reads live biometric data. The threshold value accessed from the handheld device **206** during step **1802** is used by the extraction system in reader **300** to extract live biometric data at step **1806** from the read biometric data. The extracted live biometric data is stored in the reader **300** at step **1808**. The reader **300** is coupled to a network at step **1810**, which may be via a law enforcement field computer (not shown) or the like. The threshold value, the live biometric data, and the stored biometric data are transmitted via the network to a matching system at step **1812**. Matching is performed at step **1814**, which produces (1) a result of a comparison between the stored biometric data and the live biometric data and (2) a score is based on the result and the threshold value. The score is used to verify who the individual is at step **1816**. An output is sent to the law enforcement field computer at step **1818** from the network. Thus, timely and accurate verification can be made in the field through use of the threshold value during scoring of the result.

[**0089**] The score values are a correlation between the live extracted biometric data and the stored biometric data based on the threshold value. For example, scores may range from 0 to 1000, where 500 is an acceptable score for an average individual as being a positive match, and anything below is not a positive match. The threshold value may adjust the acceptable score for a below average person to 300 in order for a match to be positive, while the threshold value may adjust the acceptable score for an above average person to 900 in order for a match to be positive. Thus, in this way each individual's biometric data is taken into consideration when determining what score is needed to allow then entry into an accessed system.

[**0090**] Remote Management Operation

[**0091**] Turning now to **FIG. 19**, a remote management operation **1900** according to embodiments of the present invention is shown. An object of an individual trying to access the accessed system **112** is detected and the system administrator **118** is notified at step **1902**. Live biometric data, stored biometric data, and other data is read at step **1904** and sent via the network **114** to the extracting system **108**. Any parameters to be used during extraction are sent from the system administrator **118** to the extracting system **108** at step **1906**. Extraction of the live biometric data is performed, and the extracted live biometric data is sent to the system administrator **118** via the network **114** at step **1908**. The extracted live biometric data, the read stored biometric data, and any matching parameters are transmitted from the system administrator **118** to the matching system **110** at step **1910**. The results from performing the matching are transmitted to the system administrator **118** at step **1912** via the network **114**. The system administrator **118** performs access control of the accessed system **112** based on the matching results at step **1914**. After performing the access control, the method **1900** returns to step **1902** to wait for another object to be detected.

[**0092**] With reference to **FIG. 20**, a remote management operation **2000** according to other embodiments of the present invention is shown. The system administrator **118** sends commands to configure, initialize, or update the system **100** at step **2002**. The system administrator **118** sends commands to obtain information from elements within the system **100** at step **2004**. The information may be audit information, log information, status information, polling information, or the like. The system administrator **118** sends event commands at step **2006**. This may be when there is an emergency, when fire access is required, when an individual is not allowed into an accessed system **112**, or the like.

[**0093**] In these embodiments utilizing a system administrator **118**, small organizations that need external support for their access control or large organizations that need a central or remote station for their access control can utilize a network, such as the Intranet or the Internet, as part of their access control system **100**. For a small company, this helps reduce some costs involved in installing and maintaining an access control system. While in large companies this gives central station information about every single thing requiring access control in a company, such that problems can be detected and resolved timely.

[**0094**] Conclusion

[**0095**] While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. It will be apparent to persons skilled in the relevant art that various changes in form and detail can be made therein without departing from the spirit and scope of the invention. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

What is claimed is:

1. A method, comprising:

(a) reading information from a smart card of an enrollee at an access control location;

(b) transmitting the information via a network to a central processing location;

(c) generating image data from a live capture of an image of a biometric of the enrollee using a live capture device at the access control location;

(d) transmitting the image data via the network to the central processing location;

(e) accessing the image date from the central processing location to extract extraction information from the accessed image data;

(f) accessing the information from the smart card from the central processing location and the extraction information to generate a matching result through comparing the extracted information with the information from the smart card; and

(g) performing access control at the access control location via the network based on the matching result.

2. The method of claim 1, further comprising:

(h) using a system administrator at the central processing location to perform step (g).

3. The method of claim 2, wherein step (h) comprises:

using an access control device as the system administrator that compares the matching result to a threshold value.

4. The method of claim 2, further comprising:

using an operator as the system administrator that reviews the matching results against a threshold value.

5. The method of claim 2, wherein:

step (f) further comprises determining a threshold quality value of the enrollee from the information on the smart card; and

step (g) further comprises using the threshold quality value and the matching result to perform the access control.

6. The method of claim 2, wherein step (h) further comprises:

using the system administrator to at least one of initialize, configure, or update at least one or more devices utilized to perform steps (a)-(g).

7. The method of claim 2, wherein step (h) further comprises:

using the system administrator to access at least one of audit information, log information, status information, or polling information from one or more devices utilized to perform steps (a)-(g).

8. The method of claim 2, wherein step (h) further comprises:

using the system administrator to transmit one or more event commands to one or more devices used to perform steps (a)-(g).

9. The method of claim 1, wherein before step (e) the central processing location monitors a plurality of extraction locations coupled the network and chooses one of the plurality of extraction locations at which to perform step (e).

10. The method of claim 1, wherein before step (f) the central processing location monitors a plurality of matching locations coupled to the network and chooses one of the plurality of matching locations at which to perform step (f).

11. The method of claim 1, wherein:

before step (e) the central processing location monitors a plurality of extraction locations coupled the network and chooses one of the plurality of extraction locations at which to perform step (e); and

before step (f) the central processing location monitors a plurality of matching locations coupled to the network and chooses one of the plurality of matching locations at which to perform step (f).

12. A distributed system for access control, comprising:

a reader that reads information from a smart card of an enrollee at an access control location;

a transmitter that transmits the information via a network to a central processing location;

an image generator that generates image data from a live capture of an image of a biometric of the enrollee using a live capture device at the access control location;

a transmitter that transmits the image data via the network to the central processing location;

an extraction service that accesses the image date from the central processing location to extract extraction information from the accessed image data;

a matching service that accesses the information from the smart card from the central processing location and the extraction information from the central processing location to generate a matching result through comparing the extracted information with the information from the smart card; and

an access controller at the access control location that controls access via the network based on the matching result.

13. The system of claim 12, further comprising:

a system administration device at the central processing location coupled to the access controller.

14. The system of claim 13, wherein the system administration device at least one of initializes, configures, or updates at least one or more of the means coupled to the network.

15. The system of claim 13, the system administration device accesses at least one of audit information, log information, status information, or polling information via the network.

16. The system of claim 13, wherein the system administration device transmits one or more event commands via the network.

17. The system of claim 12, further comprising:

a selector that selects the extraction service from a plurality of extraction locations coupled the network.

18. The system of claim 12, wherein:

the matching service a threshold quality value of the enrollee from the information on the smart card; and

the access controller uses the threshold quality value and the matching result to perform the access control.

19. The system of claim 12, further comprising:

a selector that selects the matching service from a plurality of matching locations coupled the network.

20. The system of claim 12, further comprising:

a first selector that selects the extraction service from a plurality of extraction locations coupled the network; and

a second selector that selects the matching service from a plurality of matching locations coupled the network.

* * * * *