(12) STANDARD PATENT (11) Application No. **AU 2011252761 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Automatic identity enrolment

(51) International Patent Classification(s)
G06F 19/00 (2006.01)

(21) Application No: **2011252761** (22) Date of Filing: **2011.05.13**

(87) WIPO No: **WO11/140605**

(30) Priority Data

(31) Number	(32) Date	(33) Country
2010902032	**2010.05.13**	**AU**

(43) Publication Date: **2011.11.17**
(44) Accepted Journal Date: **2016.12.15**

(71) Applicant(s)
iOmniscient Pty Ltd

(72) Inventor(s)
Bigdeli, Abbas;Lovell, Brian;Mau, Sandra

(74) Agent / Attorney
Griffith Hack, GPO Box 4164, Sydney, NSW, 2001

(56) Related Art
US 7367049 B1
US 2003/0215114 A1
US 2005/0286745 A1
US 2007/0047770 A1

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 November 2011 (17.11.2011)

PCT

(10) International Publication Number
WO 2011/140605 A1

(51) International Patent Classification:
G06F 19/00 (2011.01)

(21) International Application Number:
PCT/AU2011/000558

(22) International Filing Date:
13 May 2011 (13.05.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2010902032 13 May 2010 (13.05.2010) AU

(71) Applicant *(for all designated States except US)*: **NATIONAL ICT AUSTRALIA LIMITED** [AU/AU]; ACN 102206173, Level 5, 13 Garden Street, Eveleigh, NSW 2015 (AU).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BIGDELI, Abbas** [NZ/AU]; c/- Level 5, 13 Garden Street, Eveleigh, NSW 2015 (AU). **LOVELL, Brian** [AU/AU]; 68 York Street, Indooroopilly, QLD 4068 (AU).

(74) Agent: **FB RICE**; Level 23, 44 Market Street, Sydney, NSW 2000 (AU).

(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, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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.

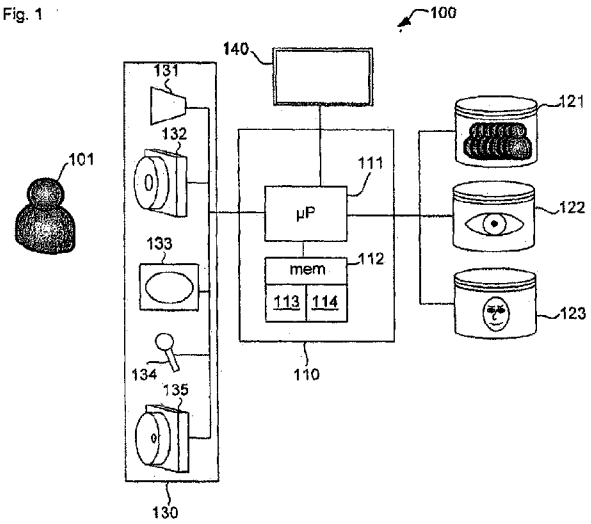
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, 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))*

(54) **Title**: AUTOMATIC IDENTITY ENROLMENT

Fig. 1



(57) **Abstract**: Biometric computer systems are systems which use one or biometric identifiers to enrol, verify or identify a person. This disclosure concerns the automatic enrolment of people into biometric systems. Aspects include methods, computer systems, software and biometric systems. A first biometric identifier (i.e. face) and a second biometric identifier (e.g. iris) is captured (201). The first biometric identifier (e.g. face) is compared (206) to the biometric identifiers associated with records in the datastore (i.e. employment records 121) to identify a candidate matching record. An association of the second biometric identifier with the candidate record to be stored (209) in memory.

WO 2011/140605 A1

2011252761 23 Nov 2016

"Automatic identity enrolment"

Technical Field

This disclosure concerns the automatic enrolment of people into biometric systems. Aspects include methods, computer systems, software and biometric systems.

Background Art

Biometric identifiers describe physiological characteristics such as iris, retina, fingerprint, hand, voice, or face. Biometric identifiers can be in the form of essentially raw data as captured by biometric sensors, or processed, such as cropped images, outliers removed or represented in feature form such as a feature histogram.

Biometric computer systems are systems which use one or biometric identifiers to enrol, verify or identify a person. The terms enrol, and register and populate will be used interchangeably throughout this document.

Use of biometrics and multimodal biometrics in biometric systems for access control, verification or identification are increasingly applied to border protection as well as private property access. However, the migration to such biometric systems for a large organisation can be expensive and time consuming due to the large number of people to enrol into the database used by the biometric computer system.

Currently, human operators are needed to manually link a person’s biometric signature (comprised of one or more biometric identifiers) to his/her existing employee record. This is however a very costly process. Not only does it cost money to hire people to operate and coordinate the enrolment process, the time lost from employees delayed or taken away from their work to pose for enrolment can also be a significant cost.

An alternative to manual enrolment is to enrol the biometric signature using an existing non-biometric verification instrument, such as an existing swipe, magnetic, or RFID card. In a card-based electronic access control system for example, a card is issued to every user enrolled in the system. The user presents his or her card to a card reader. The reader is usually connected to a controller and a host computer, which can be programmed to identify the user based on the read code. After the user has been identified, information from his/her record can be used to enrol their obtained biometric signature.

2011252761 23 Nov 2016

Any discussion of documents, acts, materials, devices, articles or the like which has been included in the present specification is not to be taken as an admission that any or all of these matters form part of the prior art base or were common general knowledge in the field relevant to the present invention as it existed before the priority date of each claim of this application.

Summary

In a first aspect there is provided a computer implemented method of automatically associating a second biometric identifier with a records stored in a datastore, wherein each record represents a person and is already associated with at least one biometric identifier of the person, the method comprising:

(a) receiving or accessing a first biometric identifier and a second biometric identifier, wherein the first and second biometric identifiers represent the same person;

(b) comparing the first biometric identifier to the biometric identifiers already associated with records in the datastore to identify a candidate matching record; and

(c) causing an association of the second biometric identifier with the candidate record to be stored in memory, whereby the candidate record is enhanced with further biometric information.

The method takes advantage that many datastores exist that represent sets of people and include biometric identifiers for each person. The method exploits this feature to automatically verify a person's identity and enhance that person's record with further biometric information that can then be used in computer implemented biometric systems. It is an advantage that this datastore can be enhanced without the use of a non-biometric verification instrument, such as an existing swipe, magnetic, or RFID card or personal identification number that would need to be entered to make the association in step (c). Since secondary verification instruments are not required this decreases the chances of fraud from users stealing those verification instruments.

The method may further comprise determining a level of confidence in the candidate matching record, such as a threshold, and only performing step (c) if the level of confidence is satisfactory.

Step (b) may further comprise determining a level of confidence in the candidate matching record, and if a candidate matching record is not identified to a satisfactory

2011252761 23 Nov 2016

level of confidence, repeating steps (a) and (b) until the satisfactory level of confidence is reached.

Alternatively, step (b) further comprises repeating steps (a) and (b) until a maximum number of repeats is reached or the end of predetermined time period is reached.

The method may comprise receiving or accessing a further instance of a first biometric identifier and second biometric identifier representing the same person and comparing each instance of the first biometric identifier to the biometric identifiers associated with records in the datastore to identify a candidate matching record. It is an advantage of the method that the identity of the person can be verified by using multiple instances of the first biometric identifier which will improve the accuracy of the matching process, and in turn accuracy in the association in step (c).

Further instances of the first and second biometric identifier are identified (i.e. as belonging to the same person) by comparison to previously received or accessed first and second biometric identifiers to identify matches.

Comparing each instance of the first biometric identifier may comprise comparing a combined representation of each instance of the first biometric identifier to the biometric identifiers associated with records in the datastore. The combined representation is based on a fusion of the instances of the first biometric identifiers, such as a fusion in feature space.

The combined representation may be based on clustering the instances of the first biometric identifiers and comparing the cluster to the biometric identifiers associated with the records in the datastore. The clustering may also be based on the second biometric identifiers.

After step (a) the method may comprise the step of determining whether at least the second biometric identifier is already associated with a record of the datastore, and if so not performing step (b) and (c).

The first biometric identifier and the second biometric identifier may be of different types.

2011252761 23 Nov 2016

The method may further comprise a first step of capturing the first biometric identifier and second biometric identifier. Capturing may not require active involvement of the user.

The biometric identifiers may be received from biometric sensors or accessed from local or remote memory which may be separate to the memory referred to in step (c). The method may be performed in real time. Step (c) may comprise storing the association in a second datastore.

The biometric identifiers can include biometric data as captured by biometric sensors, and/or processed biometric data, such as cropped images or feature histograms.

The at least one biometric identifier already associated with each record may be representative of the face of the person. In turn, the first biometric identifier may be based on an image captured of the face of the person.

Alternatively, the first biometric identifier can be any existing biometric identifier already stored in the datastore that can be used for identity verification to associate a new type of biometric identifier to the record.

The biometric identifier may be representative of one or more physiological feature of the person.

Step (c) may further comprise causing an association of the first biometric identifier with the candidate record to be stored in memory. Optionally, each instance of the first and second biometric identifier may be associated with the candidate record. Optionally a third biometric identifier may be received or accessed in step (a) that is also associated with the candidate record in step (c). This has the advantages of improving the depth and therefore future useable accuracy of the biometric information stored.

The second identifier may be a more accurate type of biometric identifier of a person than the first identifier.

The first identifier may be a representation of the iris of the person.

2011252761 23 Nov 2016

The datastore may be employee records or records of personnel allowed access to a physical area.

Associating the second biometric identifier to the candidate record may be taken to be enrolment of the person into a computer controlled biometric system. The method may be performed during an enrolment period for the computer controlled biometric system.

It is an advantage of at least one embodiment of the method that specific task personnel are not needed to enrol users into the biometric system. Further since the biometric identifiers can be captured from the user without their active involvement, such as simply walking past the sensors without needing to interact with the sensors, the method is simple without the need for training.

In a second aspect there is provided software, that is computer readable medium that when read and executed by a computer causes the computer to operate in accordance with the method described above.

In a third aspect there is provided a computer system to automatically associate a second biometric identifier with a record stored in a datastore, the system comprising:

a processor;

a datastore comprised of records, wherein each record represents a person and is already associated with at least one biometric identifier of the person;

an input port to receive or memory for the processor to access a first biometric identifier and a second biometric identifier, wherein the first and second biometric identifiers represent the same person; and

the processor to compare the first biometric identifier to the biometric identifiers already associated with records in the datastore to identify a candidate matching record, and to cause an association of the second biometric identifier with the candidate record to be stored in memory, whereby the candidate record is enhanced with further biometric information.

In a fourth aspect there is provided a biometric system using associations stored in memory according to the method described above.

Optional features of the first aspect of the invention are of course optional features of the second, third and fourth aspects of the invention.

2011252761 23 Nov 2016

Brief Description of Drawings

An example will be described with reference to:

Fig. 1 illustrates a computer system 100 for automatically populating existing database records (of say employees) with biometric information.

Fig. 2 illustrates a method 200 for automatically populating existing database records (of say employees) with biometric information.

Fig. 3 illustrates determining a combined minimum distance between captured face images and face images from a reference face image database.

Fig. 4 illustrates determining the combined distance in the feature space.

Best Mode

Fig. 1 illustrates a computer system 100 for automatically populating existing database records (of say employees) with biometric information from a person 101.

The computer system comprises a controller 110 including a processor 111 and a memory 112. The memory is divided into program code memory 114 and data memory 113. The controller 110 is connected to a reference face image database 121 that associates each face to a face id. In one example the face id is identical the employee id of the employee with that face and in that sense is an existing employee database. The controller 110 is also connected to an iris image database 122 that relates each iris image to an iris id. The iris image database 122 also records whether a particular iris has been enrolled, i.e. linked/associated to one employee id. The controller 110 is also connected to a captured face image database 123. Each database 121, 122 and 123 is stored in memory of the controller 110 that can be either local or remote to the controller.

The controller 110 is further connected by an input port to a biometric input device 130. The biometric input device comprises several biometric sensors such as face image camera 131, iris scanner 132, fingerprint scanner 133, microphone 134 and retina scanner 135. The controller is also connected to an operator interface 140. The operator interface 140 may be a touch sensitive screen, may comprise a separate display and a keyboard or may be any other suitable computing device.

In use, the person 101 is enrolled as the person 101 passes the biometric input device 130. During the enrolment period (the period in which biometric identifiers are saved

2011252761 23 Nov 2016

to the database and associated with a person), the computer system 100 captures multiple biometric identifiers over one or more observations with at least one biometric identifier already existing in a database.

In this example, the biometric input device is installed at the portal of an office building. As the person 101 passes by, at least two biometric identifiers are captured. In one example, these two identifiers are the face and the iris of the person 101. A face image and an iris image are captured by the face image camera 131 and the iris scanner 132 respectively. The capturing is orchestrated by processor 111 executing instructions of a software stored on program code memory 114.

Fig. 2 illustrates a method 200 performed by the processor 111 again executing instructions of a software program stored on program code memory to automatically populate existing database records (of say employees) with biometric information. In this example, it is assumed that a company has a reference face image database with face images from all employees. A second biometric identifier, in this example the iris image, is used and the aim is to associate a biometric identifier of the iris image to the respective employee. The required types of biometric identifiers to be linked depend on the needs of the access control system (for example, multimodal biometric access control systems may link both iris and face to the employee or may capture and store a third or fourth biometric identifier). In other examples, other combinations of biometric identifiers may be used, such as a fingerprint needs to be linked to an existing voice sample of an employee or a retina image may be used instead of the iris image.

The method is most effective if the same person walking past a second time is recognised as the same person as before. Therefore, the second biometric identifier, or a combination of biometric identifiers, needs to provide reliable matching. In this example, the iris image is used as such a biometric identifier for matching instances of biometric identifers of the same person.

The method 200 commences by capturing 201 an iris image and a face image of a person 101. The captured iris image (or representation of the images) is matched 202 against the irises saved in the iris image database 122 to find the iris id of the iris that best matches the captured iris image.

2011252761 23 Nov 2016

If the person is passing by for the first time, the captured iris image will not find a match in the iris image database 122. In that case, the iris image is stored in the iris image database 122 with an associated new iris id, and the captured face is also stored in the captured face image database 123 associated with the new iris id. The captured face image is compared to the records of the reference face image database 121 by computing a distance between the captured face and the faces from the reference face image database 121. If a candidate matching record is found that meets a satisfactory level of confidence, such as has a distance below a predefined threshold, then the iris image is associated with this face and the related employee id in the iris image database 122. If no match satisfies the threshold condition the method restarts at step 201.

The following describes the case of a person passing by for an additional time. In that case, the captured iris image matches an iris image in the iris image database 122. From the iris image database 122 it is determined whether the iris image has already been enrolled 204, that is an association between the iris image and an employee has already been stored, such as the employee id has been recorded with this iris image in the iris image database 122. If the iris image has already been enrolled the method 200 ends 205 here. The person may be greeted by name or notified of the successful enrolment.

If the iris has not been enrolled, the newly captured face image is stored in the face image database associated with the iris id (as determined from the look up on the iris image database at step 201). The aim is now to identify a record, that is face, from the reference face image database that best matches the all captured face images of that iris id.

Each face associated with the iris id can be compared separately and the results combined. In this example, the best match is determined by determining a combined minimum distance 206. In one example, the method used for face matching is multi-region probabilistic histogram (MRH) as described in [1]. This method employs 2-dimensional Discreet Cosine Transformation (DCT) and a statistical model to transform the face images into a feature space spanned by feature vectors. Based on these feature vectors, a distance between two face images can be determined.

Fig. 3 illustrates the determining of a combined minimum distance between captured face images and face images from a reference face image database. Four face images

2011252761 23 Nov 2016

instances 311-314 are of the same person captured under different conditions, such as by four passes of the biometric input device 110. As described above these images are grouped since they were captured together with matching irises. Each of the captured face images 311-314 is transformed into a respective feature vector 321-324 as in the MRH method. Based on the feature vectors 321-324 a combined feature vector 330 is determined.

Fig. 4 illustrates determining the combined distance in the feature space. Reference numerals in Figs. 3 and 4 correspond where they have the same last two digits. Fig. 4 shows a first feature space 420 of face image instance of one person. Solid points 421-424 represent the feature vectors 321-324 in Fig. 3. Since the feature vectors 421-424 are from the same person, they are clustered within close distance. An example of a combined feature vector 430 by calculating average MRH is located in the cluster centre of the first feature space 420.

Returning back to Fig. 3, four face images 341-344 from a reference face image database are shown together with the respective feature vectors 351-354. Combined distances 361-364 are shown between the combined feature vector 330 and the feature vectors of the faces from the reference face image database 121. A detailed explanation of how these distances are computed can also be found in [1].

Fig. 4 shows a second feature space 440 including four circles 451-454 representing the feature vectors 351-354 of faces from the reference face image database in Fig. 3. It is now apparent from Fig. 4 that the feature vector 453 of face 343 is closest to the combined feature vector 430 of the captured face images. The distance of the combined feature vector 430 to the feature vector 453 is then referred to as combined minimum distance. As a result, the record for face image 343 from the reference library is determined as the best candidate match to the captured face images 311-314. A threshold or classifier can be further used to determine whether this combined minimum distance is confident enough to associate the captured faces with the identity of the best match.

It is noted that the first feature space 420 and the second feature space in Fig. 4 are shown as disjunctive but may also be intersecting. In fact, the best match, in this example feature vector 453, may be located at or close to the location of the combined feature vector 430.

2011252761 23 Nov 2016

A different way of determining a combined minimum distance is to determine a distance between each of the feature vectors 321-322 of the captured face images 311-314 and each of the feature vectors 351-354 of the face images 341-344 from the reference face image database. From these 16 distances the smallest distance is selected. In the example of Fig. 4 this smallest distance is between feature vectors 423 and 453. Alternatively, an average is computed of the distances between the feature vectors 321-324 and one face image 341 from the reference face image database. This step is repeated for the remaining face images 342-343 from the reference face image database. From the resulting average distances the smallest average distance is selected. Referring to Fig. 4 this means that the average of distances between feature vectors 421-424 and feature vector 453 is smaller than the average distance between feature vectors 421-424 and any of the remaining feature vectors 451, 452 and 454.

It should be noted that a combination of two methods, method of feature averaging of captured faces and method of minimizing over multiple face searches, can also be used to find the closest matching identity. For example, rather than having one cluster center 430 through averaging the features, multiple cluster centers can be derived for the captured faces through feature clustering techniques such as k-means. Then with each of those cluster centers, the distances to the faces in the image database can be determined and minimum distance (and corresponding) found.

Since the method of minimum distances may be influenced by outliers and therefore less robust, the first method of determining a combined feature vector 330 is applied in the following.

The combined minimum distance is compared 208 to a threshold value. If the combined minimum distance is below the threshold the iris image database is updated 209 by associating the employee id with the iris id, in the example of Fig. 3 the employee id related to face image 343.

This completes the enrolment for this particular person. If the combined minimum distance is above the threshold more observations (i.e. instances) are required. Before the next observation is captured, it is determined 210 whether a predetermined maximum number of observations has already been processed. If the maximum number of observations has been reached, the iris image is verified 211 manually by the

2011252761 23 Nov 2016

operator. If the maximum number of iterations has not been reached, the method waits for the person to pass by 201 again and another face and iris image can be captured 202. Typically, the method would be concluded at the end of the enrolment period.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the scope of the invention as broadly described.

For example, three databases are described as used to perform the invention where in fact only as few as one database is required. For example associations between an employee and the iris image could be made directly into the reference image database where the iris image is also stored. Iris images of unidentified personnel could be stored in temporary records until associated with an employee id.

Identifying instances biometric identifiers of the same person over time is described here is based on comparing iris images alone. Better accuracy is achieved is the comparison is made on all available biometric identifiers. In this case, both the iris and face image is compared to the already captured images in the iris and face image captured database in order to identify previously captured images.

At step 202 the most recently captured iris image can also be stored in the iris database associated with the identified iris id. All the iris images associated with iris id may be then be used the next time step 202 is performed to again improve accuracy.

The computer system of Fig. 1 could be a distributed computer system.

The image of the person's face can also be associated with the employee id in the irus datastore. The example only receives two types of biometric identifiers. In alternate examples, three or more biometric identifiers could be received and then also associated with the employee id in the iris datastore. More biometric information stored, the more accurate the enrolment database is, including the number of instances of biometric identifiers it is based on and the number of types of biometric identifiers.

It should be understood that the techniques of the present disclosure might be implemented using a variety of technologies. For example, the methods described herein may be implemented by a series of computer executable instructions residing on

2011252761 23 Nov 2016

a suitable computer readable medium. Suitable computer readable media may include volatile (e.g. RAM) and/or non-volatile (e.g. ROM, disk) memory, carrier waves and transmission media. Exemplary carrier waves may take the form of electrical, electromagnetic or optical signals conveying digital data steams along a local network or a publically accessible network such as the internet.

It should also be understood that, unless specifically stated otherwise as apparent from the following discussion, it is appreciated that throughout the description, discussions utilizing terms such as "estimating" or "processing" or "computing" or "calculating", "optimizing" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that processes and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

[1] Sanderson, Conrad and Lovell, Brian C. (2009). *Multi-region probabilistic histograms for robust and scalable identity inference*. In: Massimo Tistarelli and Mark S. Nixon, Advances in Biometrics: Proceedings of Third International Conference, ICB 2009. 3rd IAPR/IEEE International Conference on Biometrics, Alghero, Italy, (199-208). 2-5 June 2009.

2011252761 23 Nov 2016

CLAIMS:

1. A computer implemented method of automatically associating a second biometric identifier with record stored in a datastore, wherein each record represents a person and is already associated with at least one biometric identifier of the person, the method comprising:

(a) receiving or accessing a first biometric identifier and a second biometric identifier, wherein the first and second biometric identifiers represent the same person;

(b) comparing the first biometric identifier to the biometric identifiers already associated with records in the datastore to identify a candidate matching record; and

(c) causing an association of the second biometric identifier with the candidate record to be stored in memory, whereby the candidate record is enhanced with further biometric information.

2. The computer implemented method according to claim 1, wherein step (b) further comprises determining a level of confidence in the candidate matching record, and if a candidate matching record is not identified to a satisfactory level of confidence, repeating steps (a) and (b) until the satisfactory level of confidence is reached.

3. The computer implemented method according to claim 1 or 2, wherein the method comprises receiving or accessing a further instance of a first biometric identifier and second biometric identifier representing the same person and comparing each instance of the first biometric identifier to the biometric identifiers associated with records in the datastore to identify a candidate matching record.

4. The computer implemented method of claim 1, 2 or 3, wherein comparing each instance of the first biometric identifier comprises comparing a combined representation of each instance of the first biometric identifier to the biometric identifiers associated with records in the datastore.

5. The computer implemented method of claim 4, wherein the combined representation is based on clustering the instances of the first biometric identifiers and comparing the cluster to the biometric identifiers associated with the records in the datastore.

6. The computer implemented method of any one of the preceding claims, wherein the first biometric identifier and the second biometric identifier are of different types.

2011252761 23 Nov 2016

7. The computer implemented method of any one of the preceding claims, wherein the at least one biometric identifier already associated with each record is representative of the face of the person.

8. The computer implemented method of any one of the preceding claims, wherein the second identifier is a more accurate type of biometric identifier of a person than the first identifier.

9. The computer implemented method of any one of the preceding claims, wherein the first identifier is a representation of the iris of the person.

10. The computer implemented method of any one of the preceding claims, wherein the datastore is employee records or records of personnel allowed access to a physical area.

11. The computer implemented method of any one of the preceding claims, wherein associating the second biometric identifier to the candidate record is taken to be enrolment of the person into a computer controlled biometric system.

12. Software, that is computer readable medium that when read and executed by a computer causes the computer to operate in accordance with the method of any one of claims 1 to 11.

13. A computer system to automatically associate a second biometric identifier with a record stored in a datastore, the system comprising:

a processor;

a datastore comprised of records, wherein each record represents a person and is already associated with at least one biometric identifier of the person;

an input port to receive or memory for the processor to access a first biometric identifier and a second biometric identifier, wherein the first and second biometric identifiers represent the same person; and

the processor to compare the first biometric identifier to the biometric identifiers already associated with records in the datastore to identify a candidate matching record, and to cause an association of the second biometric identifier with the candidate record

2011252761 23 Nov 2016

to be stored in memory, whereby the candidate record is enhanced with further biometric information.

14. A biometric system using associations stored in memory according to the method of any one of claims 1 to 11.

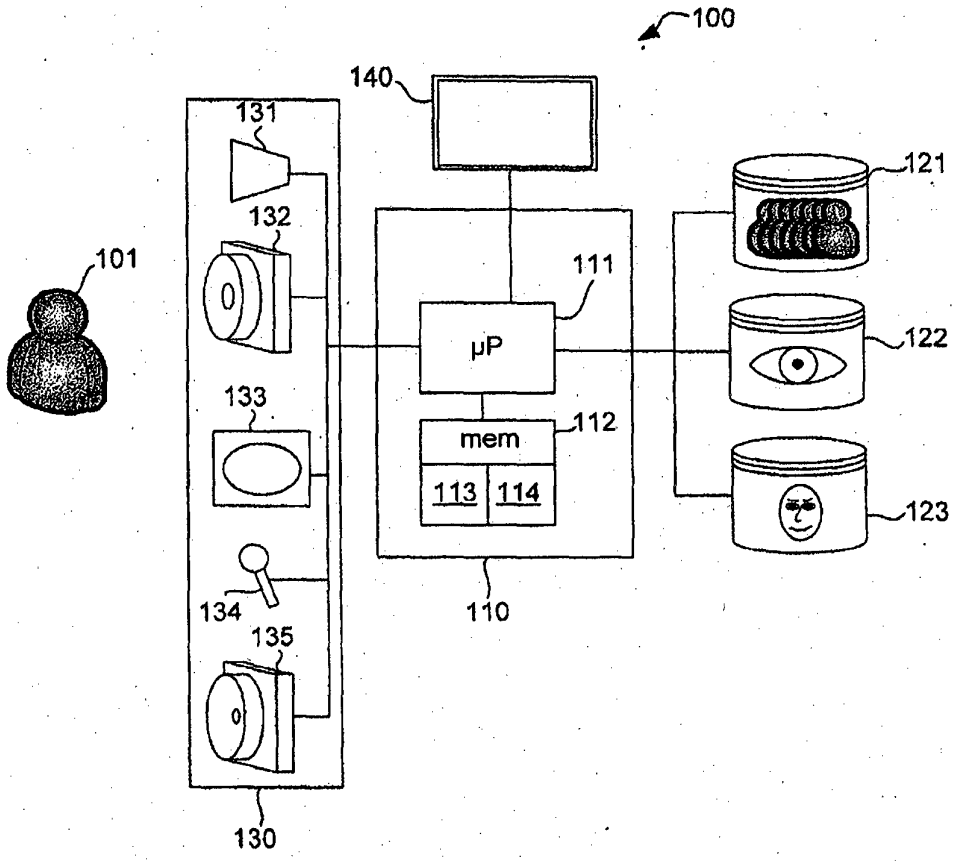

100
140
131
132
101
111
121
μP
122
133
112
mem
113
114
123
134
110
135
130

Fig. 1

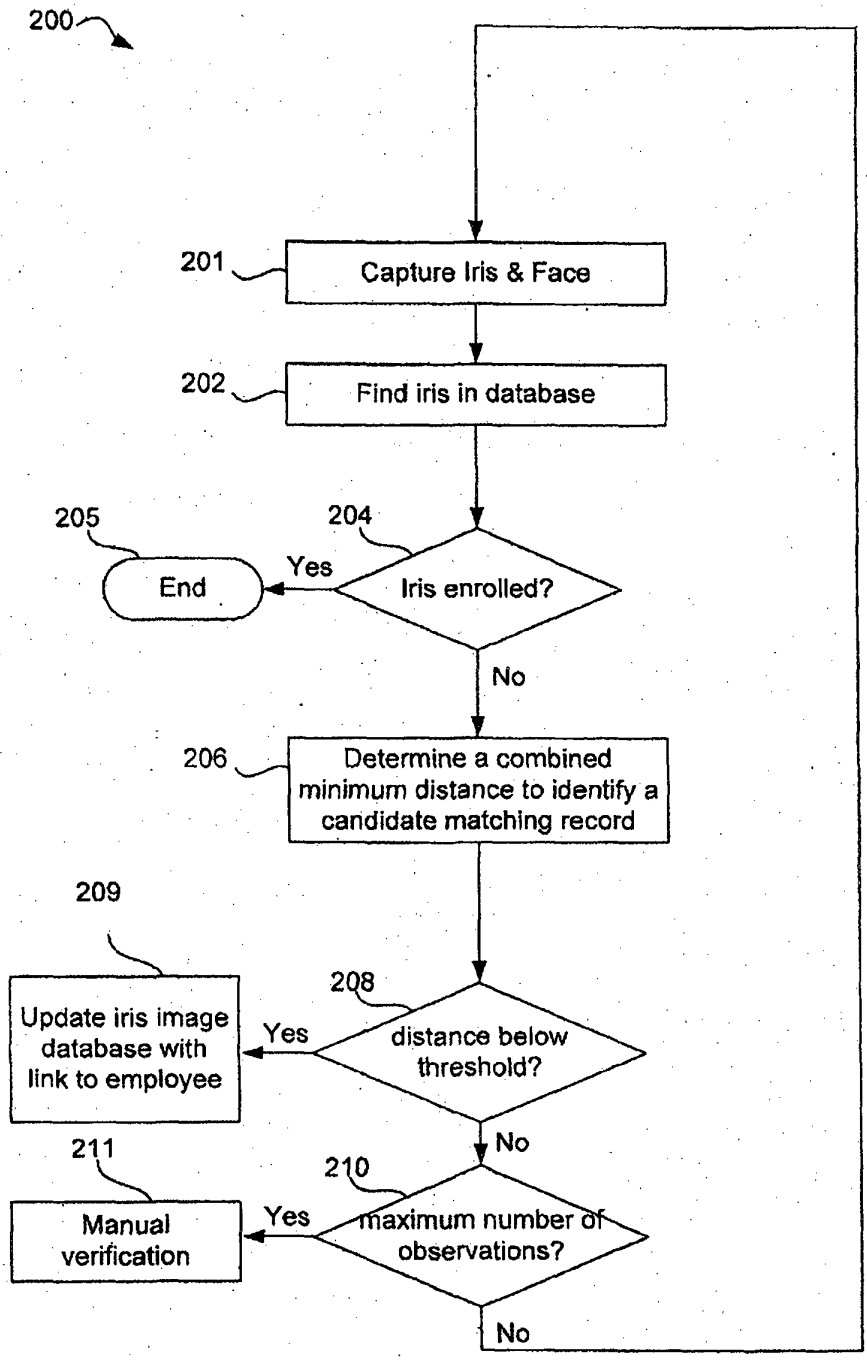

200
201
Capture Iris & Face
202
Find iris in database
205
End
Yes
204
Iris enrolled?
No
206
Determine a combined minimum distance to identify a candidate matching record
209
Update iris image database with link to employee
Yes
208
distance below threshold?
No
211
Manual verification
Yes
210
maximum number of observations?
No

Fig. 2

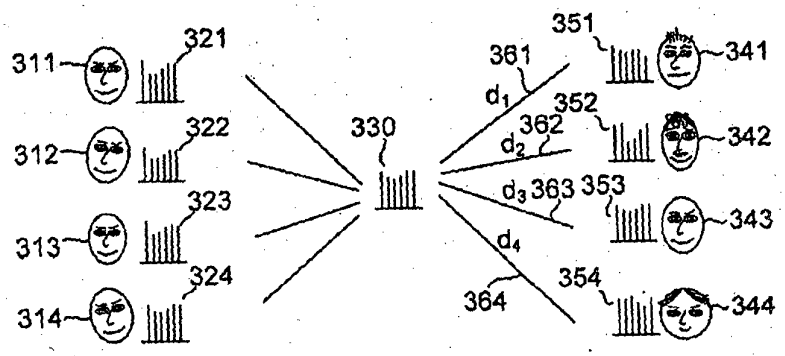

311
321
312
322
313
323
314
324
330
361
d_1
351
341
362
d_2
352
342
d_3
363
353
343
d_4
364
354
344

Fig. 3

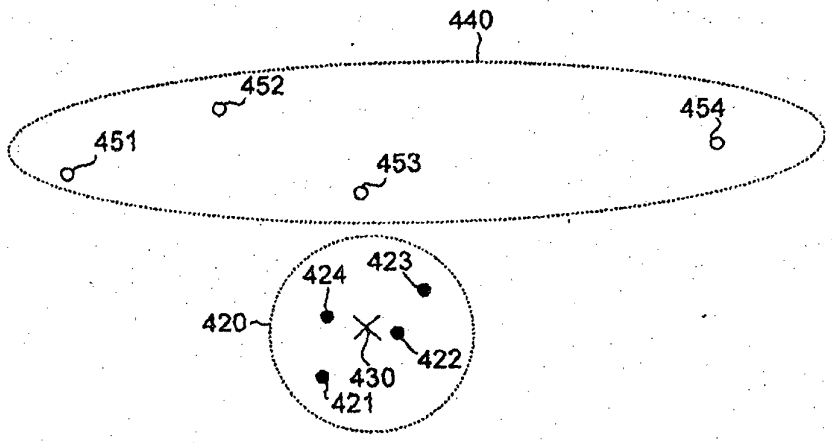

440
452
454
451
453
423
424
420
422
430
421

Fig. 4