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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
06 December 2018 (06.12.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/222304 A1

(51) International Patent Classification:
G06F 21/32 (2013.01) *H04L 29/06* (2006.01)
G06Q 20/40 (2012.01) *G06F 17/30* (2006.01)

(21) International Application Number:
PCT/US2018/029558

(22) International Filing Date:
26 April 2018 (26.04.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
17173837.0 31 May 2017 (31.05.2017) EP

(71) Applicant: **MASTERCARD INTERNATIONAL INCORPORATED** [US/US]; 2000 Purchase Street, Purchase, NY 10577 (US).

(72) Inventor: **NOWAK, Dawid**; 3 Blackwood Mews, Ongar Chase, Dublin 15 (IE).

(74) Agent: **DOBBYN, Colm, J.**; Mastercard International Incorporated, 2000 Purchase Street, Purchase, NY 10577 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

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

(54) Title: IMPROVEMENTS IN BIOMETRIC AUTHENTICATION

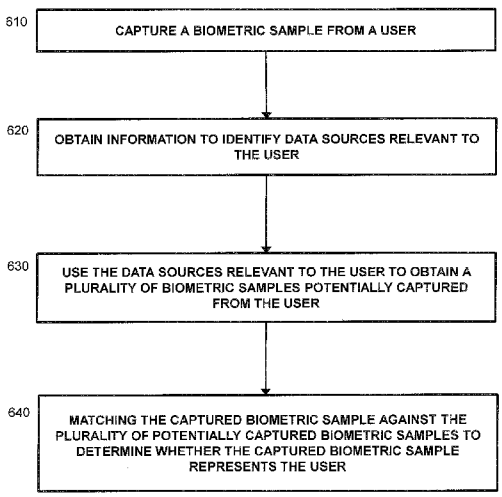

Figure 6

(57) Abstract: There is presented a method, a computing device and a biometric matching service, for the biometric authentication of a user. The method comprises capturing a biometric sample from a user and obtaining information to identify data sources relevant to the user. The method further comprises using the data sources relevant to the user to obtain a plurality of biometric samples potentially captured from the user. The method further comprises matching the captured biometric sample against the plurality of potentially captured biometric samples to determine whether the captured biometric sample represents the user.

WO 2018/222304 A1

IMPROVEMENTS IN BIOMETRIC AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATION

This application claims the benefit of, and priority to, European Patent Application No. 17173837.0 filed on May 31, 2017. The entire disclosure of the above application is incorporated herein by reference.

TECHNICAL FIELD

The present disclosure relates to improvements in biometric authentication and particularly, but not exclusively, to biometric authentication on a computing device. Aspects of the disclosure relate to a method, a computing device and a service.

BACKGROUND

Authentication is a process in which the credentials provided by a user are examined in order to confirm the identity of the user. This is usually done by comparing submitted credential values with stored credential values, typically stored in a database protected against subversion. If the submitted user credentials match those in the database, then the user is authenticated, which generally leads to a further result, such as a grant of access to a system. This type of authentication is relevant to many fields – it authorises human-to-machine interactions to enable access to systems, applications, and even resources. One field in which authentication is widely used is in transaction systems, such as for making mobile payments.

Typically, authentication is carried out through the use of usernames and PINs (personal identification numbers) or passwords. Currently, password-based authentication is not considered to provide a high enough level of security in itself for many systems that contain sensitive information. In addition, users are prone to forgetting passwords or mistakenly entering the incorrect password resulting in the system becoming locked. Other authentication mechanisms are increasingly used – one such approach is biometric authentication.

Biometric authentication uses the unique biological characteristics of individuals to validate the identity of the individual for access to a system. Examples of biological characteristics that can be relied upon for biometric authentication include fingerprints, hand geometry, retina and iris patterns, face recognition, voice

waves and signatures. A biometric authentication process can be used to secure a range of electronic communications such as online banking, logging into a computer or smartphone or making payments. Typically, the biometric authentication system compares the captured biometric data to authentic data that is stored in a database. Provided the two data samples match with each other, authentication would be confirmed and access to the system would be granted.

There are currently many issues with biometric authentication systems. Recognition errors are commonplace in this field. These errors comprise two types: the false accept rate, which is when a non-matching pair of biometric data is wrongly accepted as a match by the system, and the false reject rate, which is when a matching pair of biometric data is wrongly rejected by the system.

Another important issue with biometric systems concerns attacks. To authenticate the user, a newly acquired input signal is matched against an original signal that has been previously acquired from the user and stored in a database. If the new signal matches the original signal, access to the system is granted. Unsurprisingly, there are many areas of attack in a biometric system. For example, by presenting fake biometrics or stored digitised biometrics signals. Other examples include intercepting and modifying the data that travels between the stored original signals and the matching mechanism, or corrupting the matching mechanism to product pre-selected match scores.

While face recognition is considered to be a particularly convenient form of biometric authentication, there are weaknesses in current systems. Face recognition uses the spatial geometry of distinguishing features of the face to authenticate a user. However, face recognition does not always work well with poor lighting, low resolution or objects that partially cover the user's face. In addition, difficulties often arise if the user fails to look directly into the camera or if the face of the user changes with ageing. Therefore it is difficult to accurately authenticate the recognition of the user's face. Arguably the most important difficulty with face recognition software is to implement a suitable level of security for authentication processes. Therefore there is scope for improvement on current approaches to biometric authentication.

The present disclosure has been devised to mitigate or overcome at least some of the above-mentioned problems.

SUMMARY OF THE DISCLOSURE

According to an aspect of the present disclosure there is provided a method of biometric authentication of a user. The method comprises capturing a biometric sample from a user and obtaining information to identify data sources relevant to the user. The method further comprises using the data sources relevant to the user to obtain a plurality of biometric samples potentially captured from the user. The method further comprises matching the captured biometric sample against the plurality of potentially captured biometric samples to determine whether the captured biometric sample represents the user.

The biometric sample may be an image of the user's face.

The biometric sample may be obtained at a mobile computing device of a user.

Obtaining the plurality of biometric samples and matching the captured biometric sample against the plurality of biometric samples potentially captured from the user may be carried out remotely from the mobile computing device of a user.

The mobile device may be adapted to perform a mobile application, and biometric authentication may be carried out to meet a requirement of the mobile application.

The mobile application may be a mobile payment application, and the requirement of the mobile application may be performance of a transaction.

Information to identify data sources relevant to the user may comprise contacts of the user and social media account information of the user.

The method may further comprise providing information relating to user identity or behaviour, including one or more of mobile device location, user home location and user employer and work location.

The method step of obtaining a plurality of biometric samples potentially captured from the user may comprise using the captured image to obtain matching images and associated metadata from a plurality of information sources. The method step of matching the captured biometric sample against the plurality of potentially captured biometric samples may comprise comparing the information to identify data sources relevant to the user and/or the information relating to user identity or behaviour with the associated metadata.

The method step of obtaining a plurality of biometric samples potentially captured from the user may comprise analysing social networks of the user

to determine higher order contacts, and searching for images identified as being of the user by one or more of the higher order contacts.

The method of biometric authentication of a user may further comprise collating the results received for the higher order contacts. The method may further comprise calculating a confidence threshold for identifying the user as represented by the image from the images retrieved and associated metadata.

According to an aspect of the present disclosure there is provided a computing device adapted for biometric authentication of a user. The computing device may comprise at least one processor, at least one memory and a biometric capture means. The computing device may be adapted to capture a biometric sample from the user and to determine information to identify data sources relevant to the user. The computing device may be further adapted to provide the captured biometric sample and the information to identify data sources relevant to the user to a biometric matching service.

The biometric capture means of the computing device may comprise a camera and the biometric sample may be an image of the user's face.

According to an aspect of the present disclosure there is provided a biometric matching service. The biometric matching service may be adapted to receive a captured biometric sample from a user together with information to identify data sources relevant to the user;

The matching service may use the data sources relevant to the user to obtain a plurality of biometric samples potentially captured from the user.

The matching service may match the captured biometric sample against the plurality of potentially captured biometric samples to determine whether the captured biometric sample represents the user.

BRIEF DESCRIPTION OF THE DRAWINGS

One or more embodiments of the disclosure will now be described, by way of example only, with reference to the accompanying drawings, in which like components are assigned like numerals and in which:

Figure 1 illustrates schematically the relevant physical elements of a mobile computing device – in the embodiment shown, a mobile phone – in accordance with an embodiment of the disclosure.

Figure 2 illustrates schematically the software architecture of a mobile computing device, in accordance with an embodiment of the disclosure;

Figure 3 illustrates schematically method steps in a first embodiment of the disclosure;

Figure 4 illustrates schematically method steps in a second embodiment of the disclosure;

Figure 5 illustrates schematically method steps in a further embodiment of the disclosure; and

Figure 6 illustrates schematically method steps in a general embodiment of the disclosure.

DETAILED DESCRIPTION

Specific embodiments of the disclosure will be described below with reference to the Figures. The approach taken to authenticating a user is applicable to any form of computing device, but it has particular utility for mobile computing devices such as smart phones, and relevance to applications such as mobile banking. Given this relevance, Figure 1 shows the relevant physical elements of a mobile computing device in the form of a smart phone. The smart phone of Figure 1 is suitable for the implementation of embodiments of the disclosure as described with reference to Figures 2 to 6.

Figure 1 shows schematically relevant parts of a representative hardware architecture for a mobile computing device suitable for implementing an embodiment of the disclosure. In the example shown, each mobile computing device is a mobile cellular telecommunications handset ("mobile phone" or "mobile device") – in other embodiments, the computing device may be another type of computing device such as a laptop computer or a tablet and the computing device need not have cellular telecommunications capabilities.

The mobile phone (100) in Figure 1 comprises a SIM or USIM (105). The mobile phone also has a display (110) providing, in this example, a touchscreen user interface. The mobile phone (100) is equipped with a wireless telecommunications apparatus (115) for communication with a wireless telecommunications network and local wireless communication apparatus (120). A remote server (125) is also shown in Figure 1. The mobile phone (100) can be

connected to the remote server (125) by a network connection. The mobile phone also has a camera (130).

Figure 2 illustrates the software architecture of a mobile computing device, in accordance with an embodiment of the disclosure. In Figure 2, a main operating environment (205) of the mobile computing device is shown along with a protected operating environment (210). The protected operating environment may be a SIM (105). Alternatively, there may be a sandbox or other logically protected environment in the main operating environment to provide a secure environment.

The main operating environment (205) comprises an application processor (210) and associated memories (215). The main operating environment may be used with a generic operating system (such as iOS or Android). The main operating environment also comprises other applications normally needed by such a mobile computing device, such as a browser (220), a modem (225) and a camera driver (230).

The protected operating environment (240) may comprise a biometric application (245) and an application that uses the biometric application (245) for user authentication purposes. In this case, the application is a transaction application, specifically a mobile payment application (250), whereby the biometric application is called by the mobile payment application. In Figure 2, both applications are explicitly shown in the protected operating environment. The applications may be located within the SIM or within another physically or logically protected environment so that third parties can have confidence in biometric results produced by the biometric application. Alternatively, some parts of the biometric application and the mobile payment application may be situated in the protected operating environment. Further, data from one or both of these applications may be located in a protected memory.

Figure 6 shows a general embodiment of a method of biometric authentication of a user. First of all, a biometric sample is captured (610) from a user, and information is obtained (620) to identify data sources relevant to the user. These data sources relevant to the user are then used (630) to obtain a plurality of biometric samples potentially captured from the user. This is followed by matching (640) of the captured biometric sample against the plurality of potentially captured biometric samples to determine whether the captured biometric sample represents the user. The significance of each step will now be described in more detail, after which alternative embodiments will also be discussed.

In embodiments described in more detail below, the biometric sample captured from the user is a digital image of the user's face for use in a face recognition or matching process captured by camera (130). In principle, other biometrics (such as a fingerprint or a voice print) could also be captured in this way, but embodiments of the disclosure described below are particularly well adapted to using captured facial images of a user.

The biometric sample will typically be provided from the user's mobile phone (100). Typically, the mobile payment application (250) will call the biometric application (245) – in the case of facial recognition or matching with the recognition to take place offline, the biometric application (245) may simply provide a structure for capture of an appropriately framed image of the user's face. The biometric sample may then be provided to a remote server for recognition or matching to take place to allow authentication, but with additional user data collected at the same time. This additional user data will identify data sources relevant to the user that will allow the collection of biometric samples for use in recognition or matching. In the case of a user facial image as biometric, the user data may for example include social media details and contact lists. These can be used to reference images provided by the user directly to a social media account, but also images of the user tagged by a known contact, for example. The user data may also include other data (such as the user's name, or employer name) that may be used to find images of the user from public data sources with an appropriate search engine. Other user data may be provided to assist in the authentication process by confirming that the use of the device – and the making of the request – was consistent with the behaviour of the user, as will be discussed further below.

In embodiments discussed in more detail below, the interpretation of the captured biometric and its use for authentication will be carried out in a server remote from the user's mobile phone. In embodiments, however, this process may be carried out in whole or in part on the user's mobile phone, preferably in such a way that a third party can have confidence in the authentication result (with relevant processes or data secured or appropriately protected). In the approach discussed below, however, the matching or recognition process and the authentication result are achieved remotely, with an authentication result transmitted back to the user mobile phone and/or to any other system element that should receive this information, depending on the reason why authentication is required.

Different approaches to providing an authentication process according to embodiments of the disclosure will now be discussed below with references to Figures 3 to 5. These differ primarily in how the biometric samples for matching are obtained, and how the authentication process is carried out.

Figure 3 illustrates schematically method steps in a first embodiment of the disclosure. The first step is for the application to take a picture of the user's face (310). This may be prompted by the relevant mobile application at a time at which authentication of the user is needed – for example, in registering for a service, or in the case of a payment application, in instructing a mobile payment. The mobile application would then gather (320) metadata relating to the user, such as user contacts, user employer, user home or work location, and so on. This information may be obtained from the user's device, (for example from the user contact directory), or possibly from the user's social network – some of this user data may be determined in advance by the mobile application, or it may be collected at the time of image capture. The image and the user metadata is then sent (330) to a backend platform server. The image is sent to information sources on its own (hence this is termed "Blind Mode" subsequently) and used to find similar images. These information sources may simply be the corpus of information on the public internet searched by search engines, or may be information within one or another social network to which the user is subscribed. Different social networks may provide different fragments of information and metadata. For example, Facebook could provide images and social feeds, whereas Google+ could provide information on the device used, such as the current location. Similar images are obtained, together with metadata. The metadata associated with the captured image is then matched (340) to the metadata from the images retrieved from the public internet or the user's social networks. This matching of metadata is carried out in a server remote from the user's mobile phone. If there is sufficient correspondence in metadata, then the captured image is considered to be a representative image of the user, and the user may then be authenticated.

The matching of the metadata may be carried out in numerous ways. Some examples are outlined below.

Metadata may comprise any information about the user inferred from the image or a profile associated with the image. This may include, for example, geo-tagging or current location. Social networks such as Google and Facebook harvest information about the location of the user, for example the last known location or a

number of recent locations or a home location. The camera may store the location at which the image was taken. The location retrieved from social networks may then be matched with the location associated with the captured image.

Metadata may also comprise the social graph – a representation of the interconnection of relationships in an online social network – of the user. Both Google+ and Facebook have information about the social graph of a user. A list of names obtained from the social network may be compared with a list of contacts obtained from a user's device.

Metadata may also comprise information about calls that have been made and messages that have been sent from the user's device. This information may then be compared with the history retrieved from the device at the time of authentication.

Metadata may also comprise deep learning image analysis. This may involve determining background objects, such as faces, locations or monuments. For example, the face in the background may be matched with an image of the person on the contact list on the user's device.

A further matching technique may be to consider the user's Bluetooth connection history. For example, if a user's phone is synched to their car while driving, then information associated with that device and the user's relationship with that device may be used to provide additional metadata.

Figure 4 illustrates schematically method steps in a second embodiment of the disclosure. The first step is for the application to obtain a picture of the user's face (410). This may be prompted by the relevant mobile application at a time at which authentication of the user is needed – for example, in registering for a service, or in the case of a payment application, in instructing a mobile payment. The mobile application would then gather (420) metadata relating to the user, such as user contacts, user employer, user home or work location, and so on. This information may be obtained from the user's device (for example from the user contact directory) or possibly from the user's social network – some of this user data may be determined in advance by the mobile application, or it may be collected at the time of image capture. Information sources are obtained and used to find similar images (430). In this mode, the application carries out the search of the information sources. These information sources may simply be the corpus of information on the public internet searched by search engines, or may be information within one or another social

network to which the user is subscribed (this mode is termed "Social Graph" mode). Different social networks may provide different fragments of information and metadata. For example, Facebook could provide images and social feeds, whereas Google+ could provide information on the device used, such as the current location. Similar images are obtained, together with metadata. The metadata associated with the captured image is then matched (440) to the metadata from the images retrieved from the public internet or the user's social networks. This matching of metadata is carried out in a server remote from the user's mobile phone. If there is sufficient correspondence in metadata, then the captured image is considered to be a representative image of the user, and the user may then be authenticated.

Certain metadata will be used differently in the Figure 3 and Figure 4 embodiments. Some metadata may be used in the same way in both Figure 3 and Figure 4 – for matching against metadata associated with retrieved images to determine whether the images are genuinely images of the user. However, some metadata that may be used for matching in the Figure 3 arrangement may be used instead in the search of the information sources and for obtaining the retrieved images in the embodiment in Figure 4.

Figure 5 illustrates schematically method steps in a further embodiment of the disclosure. These method steps refer to the "Social graph mode" operation of the method. The first step is for the application to obtain a picture of the user's face (510). This may be prompted by the relevant mobile application at a time at which authentication of the user is needed – for example, in registering for a service, or in the case of a payment application, in instructing a mobile payment. The mobile application would then gather (520) metadata relating to the user, such as user contacts, user employer, user home or work location, and so on. This information may be obtained from the user's device (for example from the user contact directory) or possibly from the user's social network – some of this user data may be determined in advance by the mobile application, or it may be collected at the time of image capture. Information sources are obtained and used to find similar images. These information sources may simply be the corpus of information on the public internet searched by search engines, or may be information within one or another social network to which the user is subscribed (this mode is termed "Social Graph" mode). Different social networks may provide different fragments of information and metadata. For example, Facebook could provide images and social feeds, whereas

Google+ could provide information on the device used, such as the current location. The application would then obtain (530) an ordered list of contacts by frequency. One or more top contacts would then be chosen (540). The application would then search the streams of the top contacts for images of the user requiring authentication. Matching images are retrieved (550), together with metadata and the results are collated (560) by the application. The metadata associated with the captured image is then compared (570) to the metadata from the images retrieved from the public internet or the user's social networks, for example from the streams of the top contacts. A score is calculated (580) from the comparison results. The score is then compared (590) to a threshold value. If the score is above the threshold value, there is sufficient correspondence in the metadata. In this case, the captured image is considered to be a representative image of the user, and the user may then be authenticated (592). If the calculated score is below the threshold value, the statistics are updated (594).

Further embodiments of the disclosure may be provided in accordance with the scope of the disclosure as defined here.

CLAIMS

1. A method of biometric authentication of a user, comprising:

capturing a biometric sample from a user, and obtaining information to identify data sources relevant to the user;

using the data sources relevant to the user to obtain a plurality of biometric samples potentially captured from the user; and

matching the captured biometric sample against the plurality of potentially captured biometric samples to determine whether the captured biometric sample represents the user.

2. The method of claim 1, wherein the biometric sample is an image of the user's face.

3. The method of claim 1 or claim 2, wherein the biometric sample is obtained at a mobile computing device of a user.

4. The method of claim 3, wherein obtaining the plurality of biometric samples and matching the captured biometric sample against the plurality of biometric samples potentially captured from the user are carried out remotely from the mobile computing device of a user.

5. The method of claim 3 or claim 4, wherein the mobile device is adapted to perform a mobile application, and wherein biometric authentication is carried out to meet a requirement of the mobile application.

6. The method of claim 5, wherein the mobile application is a mobile payment application, and the requirement of the mobile application is performance of a transaction.

7. The method of any preceding claim, wherein information to identify data sources relevant to the user comprises contacts of the user and social media account information of the user.

8. The method of any preceding claim, further comprising providing information relating to user identity or behaviour, including one or more of mobile device location, user home location and user employer and work location.

9. The method of claim 7 or claim 8, wherein obtaining a plurality of biometric samples potentially captured from the user comprises using the captured image to obtain matching images and associated metadata from a plurality of information sources, and wherein matching the captured biometric sample against the plurality of potentially captured biometric samples comprises comparing the information to identify data sources relevant to the user and/or the information relating to user identity or behaviour with the associated metadata.

10. The method of claim 7 or claim 8, wherein obtaining a plurality of biometric samples potentially captured from the user comprises analysing social networks of the user to determine higher order contacts, and by searching for images identified as being of the user by one or more of the higher order contacts.

11. The method of claim 10, further comprising collating the results received for the higher order contacts, calculating a confidence threshold for identifying the user as represented by the image from the images retrieved and associated metadata.

12. A computing device adapted for biometric authentication of a user, comprising at least one processor and at least one memory and a biometric capture means, wherein the computing device is adapted to capture a biometric sample from the user and to determine information to identify data sources relevant to the user, wherein the computing device is further adapted to provide the captured biometric sample and the information to identify data sources relevant to the user to a biometric matching service.

13. The computing device of claim 12, wherein the biometric capture means comprises a camera and the biometric sample is an image of the user's face.

14. A biometric matching service adapted to receive a captured biometric sample from a user together with information to identify data sources relevant to the user;

wherein the matching service uses the data sources relevant to the user to obtain a plurality of biometric samples potentially captured from the user; and

matches the captured biometric sample against the plurality of potentially captured biometric samples to determine whether the captured biometric sample represents the user.

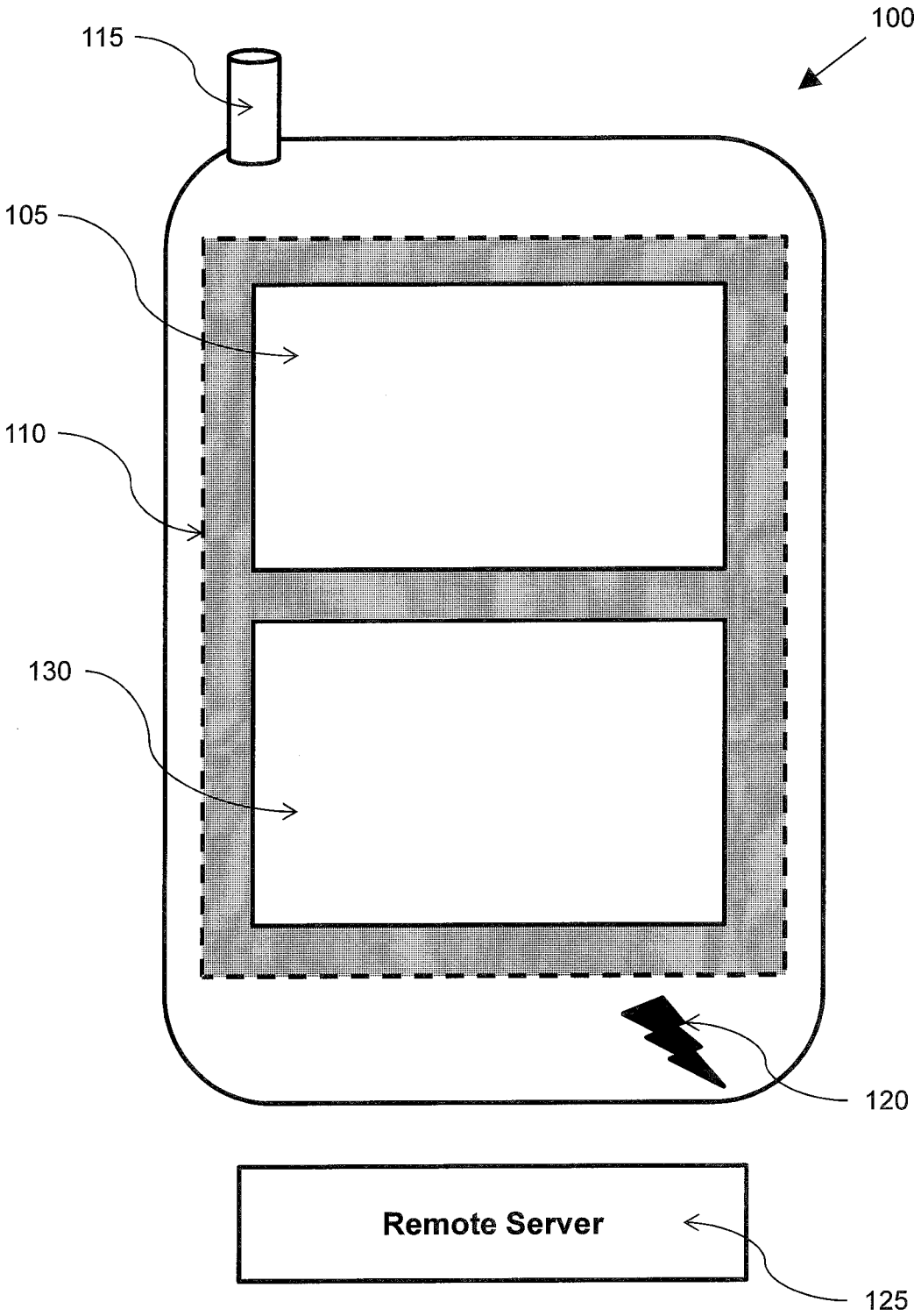

Figure 1

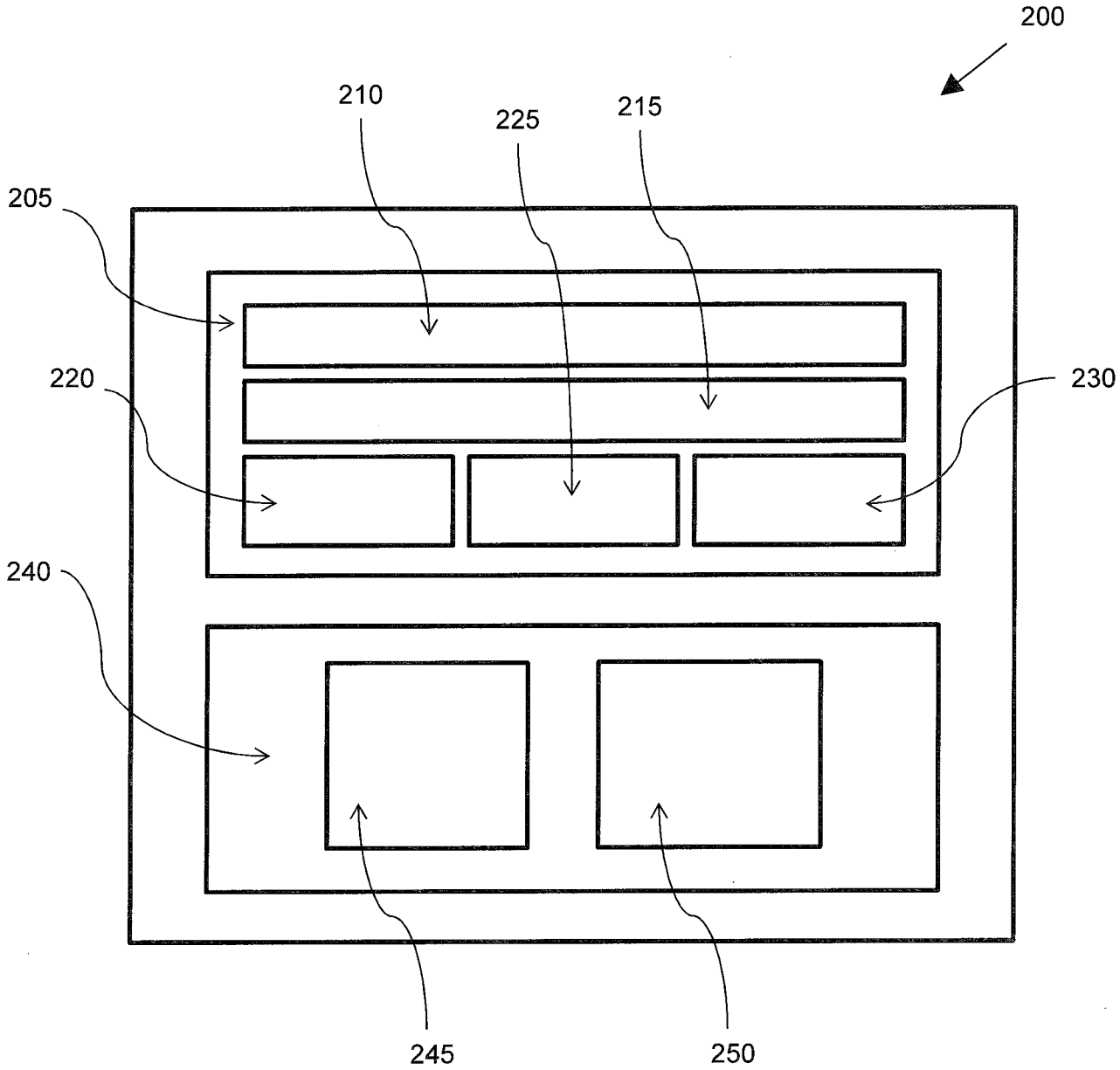

Figure 2

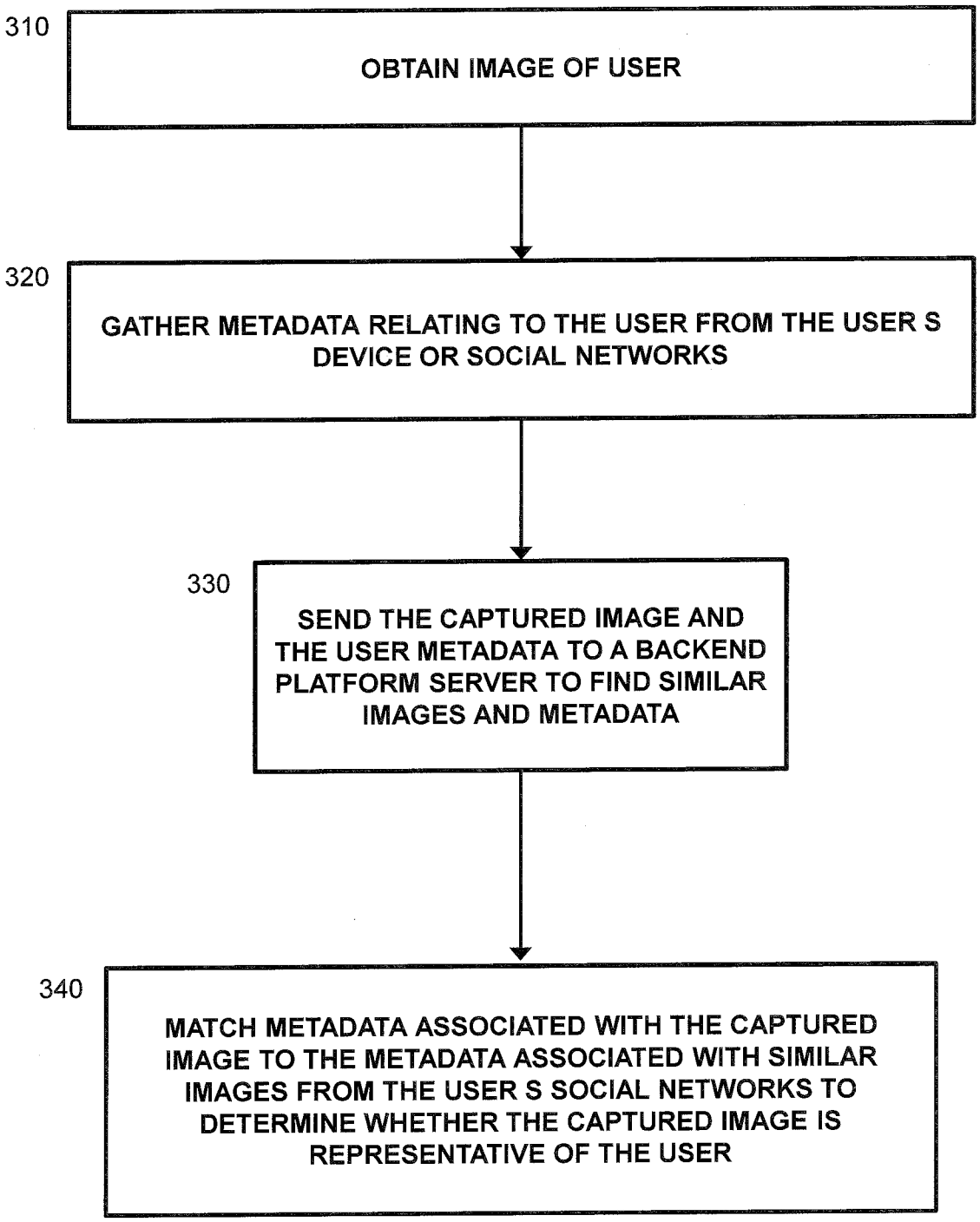
310
OBTAIN IMAGE OF USER
320
GATHER METADATA RELATING TO THE USER FROM THE USER S DEVICE OR SOCIAL NETWORKS
330
SEND THE CAPTURED IMAGE AND THE USER METADATA TO A BACKEND PLATFORM SERVER TO FIND SIMILAR IMAGES AND METADATA
340
MATCH METADATA ASSOCIATED WITH THE CAPTURED IMAGE TO THE METADATA ASSOCIATED WITH SIMILAR IMAGES FROM THE USER S SOCIAL NETWORKS TO DETERMINE WHETHER THE CAPTURED IMAGE IS REPRESENTATIVE OF THE USER

Figure 3

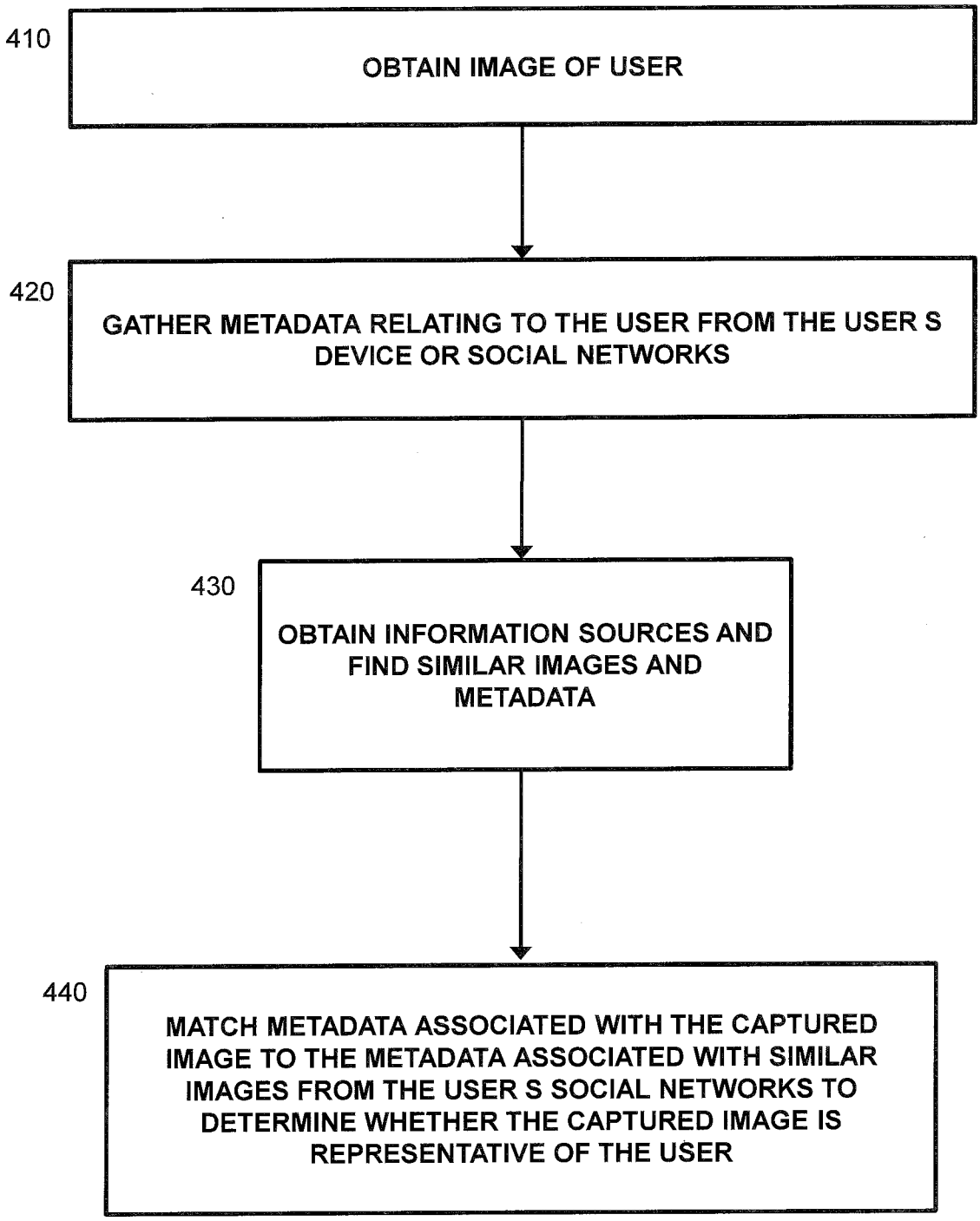
410
OBTAIN IMAGE OF USER
420
GATHER METADATA RELATING TO THE USER FROM THE USER S DEVICE OR SOCIAL NETWORKS
430
OBTAIN INFORMATION SOURCES AND FIND SIMILAR IMAGES AND METADATA
440
MATCH METADATA ASSOCIATED WITH THE CAPTURED IMAGE TO THE METADATA ASSOCIATED WITH SIMILAR IMAGES FROM THE USER S SOCIAL NETWORKS TO DETERMINE WHETHER THE CAPTURED IMAGE IS REPRESENTATIVE OF THE USER

Figure 4

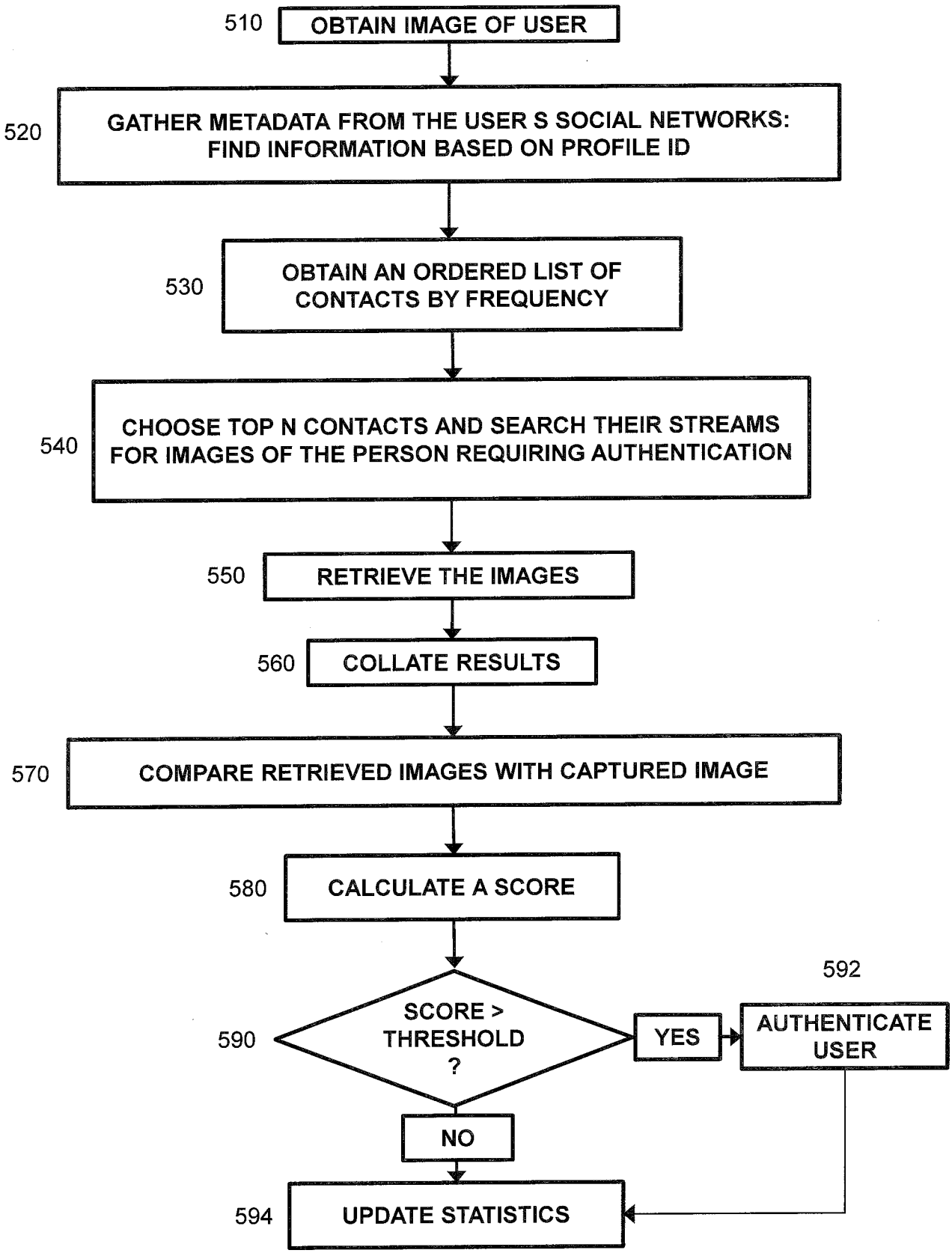
510
OBTAIN IMAGE OF USER
520
GATHER METADATA FROM THE USER S SOCIAL NETWORKS: FIND INFORMATION BASED ON PROFILE ID
530
OBTAIN AN ORDERED LIST OF CONTACTS BY FREQUENCY
540
CHOOSE TOP N CONTACTS AND SEARCH THEIR STREAMS FOR IMAGES OF THE PERSON REQUIRING AUTHENTICATION
550
RETRIEVE THE IMAGES
560
COLLATE RESULTS
570
COMPARE RETRIEVED IMAGES WITH CAPTURED IMAGE
580
CALCULATE A SCORE
590
SCORE > THRESHOLD ?
YES
592
AUTHENTICATE USER
NO
594
UPDATE STATISTICS

Figure 5

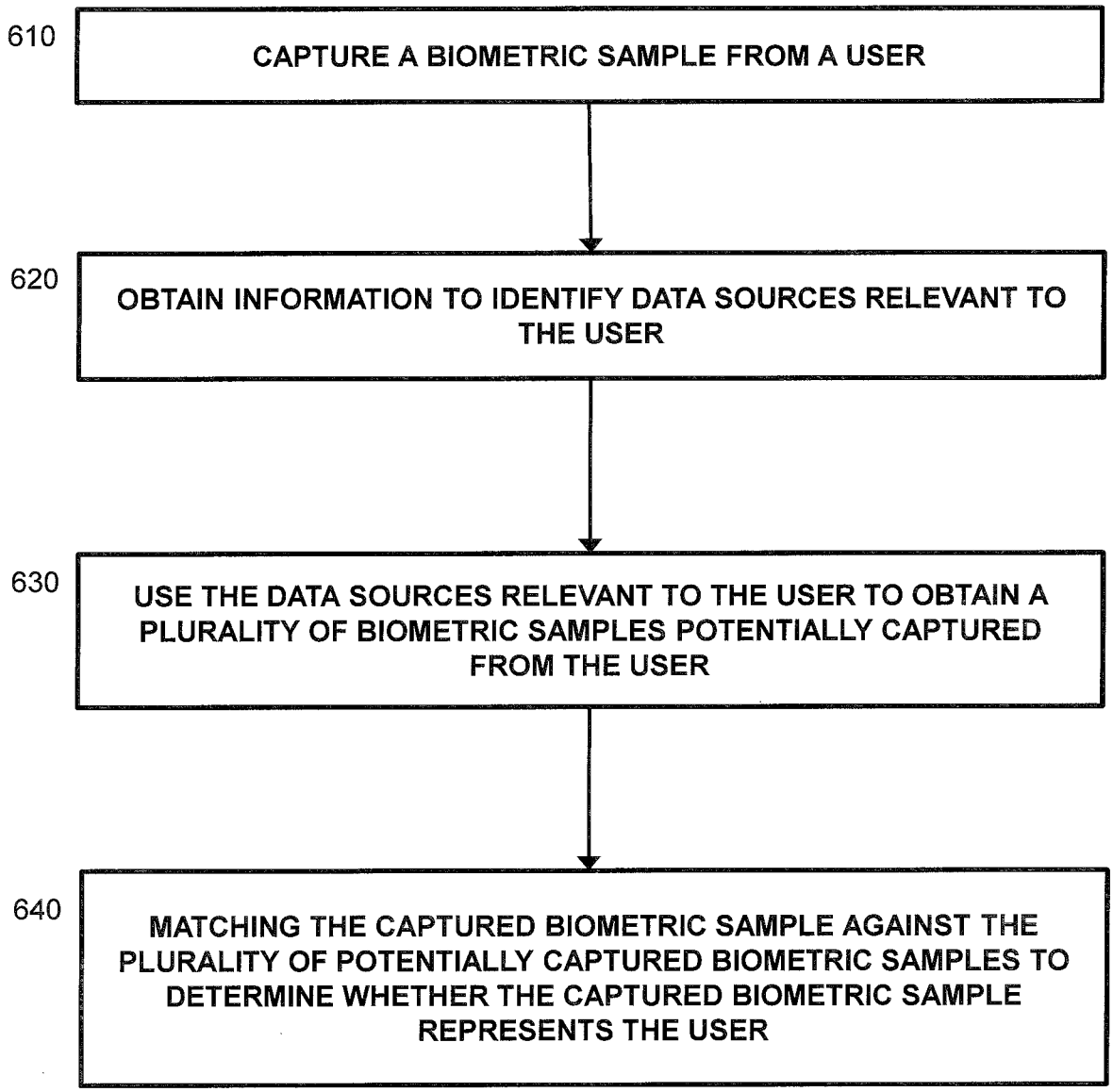
610
CAPTURE A BIOMETRIC SAMPLE FROM A USER
620
OBTAIN INFORMATION TO IDENTIFY DATA SOURCES RELEVANT TO THE USER
630
USE THE DATA SOURCES RELEVANT TO THE USER TO OBTAIN A PLURALITY OF BIOMETRIC SAMPLES POTENTIALLY CAPTURED FROM THE USER
640
MATCHING THE CAPTURED BIOMETRIC SAMPLE AGAINST THE PLURALITY OF POTENTIALLY CAPTURED BIOMETRIC SAMPLES TO DETERMINE WHETHER THE CAPTURED BIOMETRIC SAMPLE REPRESENTS THE USER

Figure 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2018/029558

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/32 G06Q20/40 H04L29/06 G06F17/30
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F G06Q G06K G07C H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2017/091533 A1 (MARDIKAR UPENDRA [US]) 30 March 2017 (2017-03-30) paragraph [0017] - paragraph [0018] paragraph [0021] - paragraph [0033] figures 1-3	1-14

X	US 2016/132671 A1 (BUD ANDREW [GB]) 12 May 2016 (2016-05-12)	1
A	paragraph [0014] - paragraph [0015] paragraph [0047] - paragraph [0051] paragraph [0055] - paragraph [0058] figures 1-4	2-14

A	US 2016/171291 A1 (PAPAKIPOS PHAEDRA [US] ET AL) 16 June 2016 (2016-06-16) paragraph [0015] column 0025 - column 0026 paragraph [0030]; figures 1-7	1-14

	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 June 2018	13/06/2018

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Hou, Jie

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2018/029558

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016/055182 A1 (PETROU DAVID [US] ET AL) 25 February 2016 (2016-02-25) paragraph [0048] paragraph [0071] paragraph [0161] figures 1-18 -----	1-14

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2018/029558

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2017091533 A1	30-03-2017	NONE	
US 2016132671 A1	12-05-2016	GB 2543117 A	12-04-2017
		GB 2543673 A	26-04-2017
		US 2013219480 A1	22-08-2013
		US 2015256536 A1	10-09-2015
		US 2016132671 A1	12-05-2016
		US 2016154953 A1	02-06-2016
		US 2016191518 A1	30-06-2016
		US 2016337350 A1	17-11-2016
		US 2017200053 A1	13-07-2017
		US 2018060681 A1	01-03-2018
US 2016171291 A1	16-06-2016	AU 2012238085 A1	26-09-2013
		BR 112013024048 A2	13-12-2016
		CA 2829079 A1	04-10-2012
		CN 103477350 A	25-12-2013
		JP 6030117 B2	24-11-2016
		JP 2014518573 A	31-07-2014
		KR 20140019807 A	17-02-2014
		MX 342076 B	13-09-2016
		US 2012250950 A1	04-10-2012
		US 2016171291 A1	16-06-2016
		WO 2012134756 A2	04-10-2012
US 2016055182 A1	25-02-2016	AU 2010279248 A1	15-03-2012
		CA 2770239 A1	10-02-2011
		CN 102667763 A	12-09-2012
		CN 104021150 A	03-09-2014
		EP 2462522 A1	13-06-2012
		JP 5557911 B2	23-07-2014
		JP 5985535 B2	06-09-2016
		JP 2013501978 A	17-01-2013
		JP 2014194810 A	09-10-2014
		JP 2016201135 A	01-12-2016
		KR 20120058539 A	07-06-2012
		KR 20160108832 A	20-09-2016
		KR 20160108833 A	20-09-2016
		US 2011038512 A1	17-02-2011
		US 2014172881 A1	19-06-2014
		US 2016055182 A1	25-02-2016
		WO 2011017653 A1	10-02-2011