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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 September 2017 (21.09.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/157435 Al

(51) International Patent Classification:
G06F 21/62 (2013.01)

(21) International Application Number:
PCT/EP2016/055726

(22) International Filing Date:
16 March 2016 (16.03.2016)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **DEUTSCHE TELEKOM AG** [DE/DE]; Friedrich-Ebert-Allee 140, 53113 Bonn (DE).

(72) Inventors: **HUI, Pan;** 1 University Road Apartment 29, HKUST, Clear Water Bay, Hong Kong (CN). **SHU, Jiayu;** 1 University Road Apartment 29, HKUST, Clear Water Bay, Hong Kong (CN). **LIU, Xin;** 1 University Road Apartment 29, HKUST, Clear Water Bay, Hong Kong (CN). **PEYLO, Christoph;** Nordweg 14, 49401 Damme (DE).

(74) Agent: **VOSSIUS & PARTNER;** Patentanwalte Rechtsanwalte mbB, SiebertstraBe 3, 81675 Munchen (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available):* AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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))*

WO 2017/157435 A1

(54) Title: A METHOD AND SYSTEM FOR VISUAL PRIVACY PROTECTION FOR MOBILE AND WEARABLE DEVICES

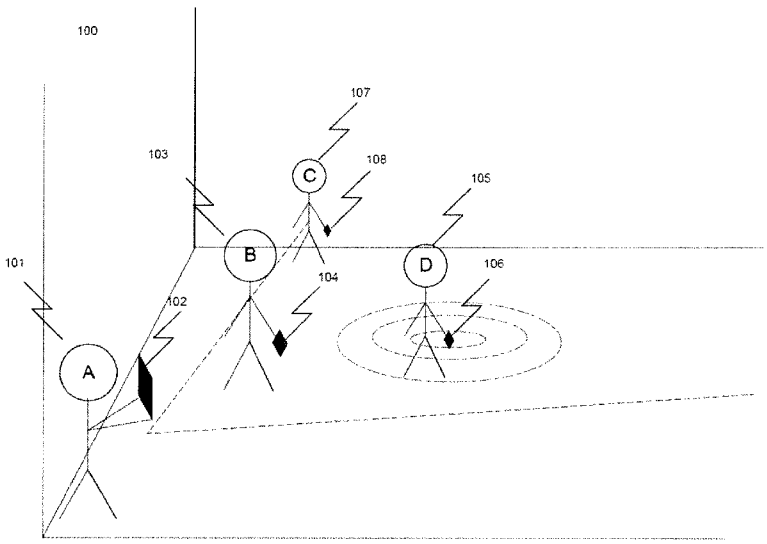

Figure 1

(57) Abstract: A method for visual privacy protection of individuals in a network with at least one first mobile device and at least one second mobile device, the mobile devices having at least one camera, the mobile devices being connected to each other within the network and/or having a direct wireless connection and the method comprising the steps of the second mobile device receiving at least one visual privacy protection request from the first mobile device, the second mobile device processing the information contained in the at least one visual privacy request using a second database on the second mobile device, the second mobile device processing acquired camera data using the information contained in the second database, and the second mobile device providing processed acquired camera data to a screen and/or outputting the processed acquired camera data to at least one application preferably running on the second mobile device.

A Method and System for Visual Privacy Protection for Mobile and Wearable Devices

The present invention generally relates to a method and system for protection mechanism for visual privacy in mobile and wearable computing devices, especially when equipped with digital cameras. In particular, the present invention relates to a method and system for providing visual privacy preserving service for mobile and wearable computing devices that are equipped with at least one digital camera.

Mobile devices with photo capturing and/or video recording functionality, for example smart phones, are ubiquitous in the modern society. Furthermore, an increasing trend in the percentage of smart phone ownership is predicted. Moreover, wearable devices, a specific type of mobile devices which incorporate a camera and permit unobtrusive picture capturing and/or videotaping, have been developed rapidly in recent years. Products, e.g., "Google Glass TM", have drawn considerable public attention.

However, the proliferation of these devices with photo capturing and/or video recording functionality, especially mobile and wearable devices can perform visual information collection unobtrusively, i.e., the above mentioned photo capturing and/or video recording. This increases the potential risk of non-consented personal information disclosure. The risk is dramatically increasing due to the improvements in performance of face recognition technology, which makes it likely to reveal one's identity from a facial image, by extracting the feature data and comparison with existing images in a database. Malicious users can utilize various visual analysis approaches to invade the privacy of those who do not intend to appear in photos or videos secretly taken.

Apprehension on unnoticeable and/or unauthorized visual information collection has been unignorably aroused from the general public. Privacy issues raised by unnoticeable visual information collection may presumably obstruct the developing wearable devices industry and remain to be solved.

It is an object of the invention to provide a method and a system for a visual privacy protection for mobile and wearable computing devices in particular to protect the privacy of individuals while preserving sufficient information. This object is achieved with the subject-matter of the independent claims. The dependent claims relate to further aspects of the invention.

The present invention provides a visual privacy protection for wearable and mobile devices, such as smart phones and smart glass.

Privacy concerns over the ubiquity of cameras can be addressed if the faces of those who do not intend to be included in the photo or video are de-identified. For de-identified faces, face recognition cannot be performed or will surely return incorrect results, and the de-identification process cannot be reversed. Notwithstanding, it is hard to distinguish which face is not supposed to be in the image or video in a specific situation, and of course it is not feasible to de-identify all existing faces. A privacy protection control has to provide the selectivity over whether an individual wants to appear in one visual file or not.

In one aspect of the invention a method for visual privacy protection of individuals in a network with at least one first mobile device and at least one second mobile device is provided. The mobile devices having at least one camera, the mobile devices being connected to each other within the network and/or having a direct wireless connection. The method comprises the steps of:

A) the second mobile device receiving at least one visual privacy protection request from the first mobile device,

B) the second mobile device processing the information contained in the at least one visual privacy request using a second database on the second mobile device;

C) the second mobile device processing acquired camera data using the information contained in the second database;

D) the second mobile device providing processed acquired camera data to a screen and/or outputting the processed acquired camera data to at least one application preferably running on the second mobile device.

In another aspect of the invention the visual privacy request comprises face representation information of an individual to be protected.

In another aspect of the invention prior to the step A) the first mobile device performs the step of generating the at least one visual privacy protection request preferably further comprising the steps of

Al) the first mobile device calculating a face representation information from a facial picture of an individual to be protected, if no previous face representation information for the individual to be protected exists in a first database of the first mobile device;

A2) the first mobile device generating a visual privacy protection request containing the face representation information of the individual to be protected and preferably further information to be sent; and/or

A3) the first mobile device further performs the step of sending the visual privacy protection request to all other devices in the network and/or in range of the direct wireless connection preferably in a predetermined time interval periodically.

In another aspect of the invention the step B) of processing the information contained in the at least one visual privacy request further comprises the steps of:

B 1) the second mobile device extracting the face representation information from the visual privacy request;

B2) the second mobile device storing face representation information in the second database in the second mobile device; and

B3) the second mobile device updating the database, if

a) a new face representation information has been extracted storing the respective face representation information, or

b) a visual privacy request has been expired, wherein

preferably determining the expiration of a visual privacy request is based on a judgment whether the second mobile device does not receive the respective visual privacy again within a predetermined period of time, as

i) the first mobile device does not send the respective visual privacy request anymore, or

ii) the first mobile device is no longer in the same network and/or in the range of the direct wireless connection.

In another aspect of the invention the step C) of processing acquired camera data using the information contained in the at least one visual privacy request further comprises the steps of:

CI) the second mobile device detecting all faces in the acquired camera data from the at least one camera;

C2) the second mobile device calculating a face representation information for each of all faces detected in the acquired camera data;

C3) the second mobile device comparing each of the calculated face representation information with the face representation information stored in the second database preferably in a pair wise fashion;

C4) the second mobile device designating each face as a face to be protected if a match is found; and

C5) the second mobile device performing a de-identification process on the acquired camera data taking into account each of the faces to be protected.

In another aspect of the invention the de-identification process of step C5) comprises at least one of the following steps:

a) altering the data of the camera input data in the region of each of the faces to be protected;

b) altering the data of the camera input data in the region of at least one of the faces to be protected by blurring the face to be protected ;

c) altering the data of the camera input data in the region of at least one of the faces to be protected by substituting the face with default data, preferably the default data being a randomly generated face; and

d) deleting the data of the camera input data in the region of at least one of the faces to be protected.

In another aspect of the invention a first mobile device is provided and configured to perform at least one of the steps of the method according any of the preceding aspects of the invention.

In another aspect of the invention a second mobile device is provided and configured to perform at least one of the steps of the method according to any one of the preceding aspects of the invention.

In another aspect of the invention a system for visual privacy protection of individuals for mobile devices is provided, the system comprising at least one first mobile device according to a previous aspect of the invention and at least one second mobile device according to a previous aspect of the invention.

In another aspect of the invention each mobile device has a privacy-preserving module and at least one of the following: a display module; a camera module; a memory management module; and a communication module.

In another aspect of the invention the respective privacy-preserving module is configured to perform the method according to any of the preceding aspects of the invention; wherein the privacy-preserving module preferably being located in a layer close to the operating system; and/or the privacy-preserving module preferably being not accessible by any third-party applications or developers; and/or the privacy-preserving module preferably being below a system services layer, preferably parallel and/or overlapping with a libraries layer.

In one embodiment of the invention a visual privacy protection system and method is provided for wearable and mobile devices, such as smart phone and smart glass. Device-to-device communication can be used to ensure visual privacy protection. Each user who currently does not wants his visual information to be collected can broadcast a specific message from his own device to all other devices nearby. In order to determine which face within the scene should be de-identified, the user should include his or her abstract facial features generated from a standard process. To ensure confidentiality, the broadcasted data cannot be used to restore the original face. Furthermore, this visual privacy protection mechanism should be implemented on the operating system level instead of a particular third-party application. Otherwise, the visual privacy protection will not be guaranteed once the user chooses not to install the particular third-party application.

In one embodiment of the invention the visual privacy protection method is mainly based on face representation information transmitted via device-to-device communication in a wireless network. The face representation information is an identification that can be used for face recognition. It is computed from face features. Therefore, the face representation information can be called abstract facial feature data. An individual who wants to protect his or her visual privacy can use a device to compute and store his or her face representation information.

In one embodiment of the invention the first mobile device initiates the connection only if the user of the first mobile intends to protect his or her visual privacy. The connection between the mobile devices is built in the form of device-to-device communication preferably in a wireless network. Then the face information of the user of the first mobile device, which is stored in the device, will be sent to the second mobile device. After the second mobile device receives the message containing any face representation information, it will save received face representation information to a database managed by the privacy protection method and keep the information for a certain period of time, i.e. the valid time. When the second mobile device obtains some visual information, all the faces in photos will be detected, and the face representation information of each face will be calculated and then compared with face representation information stored in the database. Only the face representation information within the valid time period will be used for matching faces detected in the image. Then on any matched or recognized face the de-identification operation will be performed.

According to an aspect the present invention, a method of preserving visual privacy of individuals involves at least two smart devices. The device initiating the privacy protection services comprises an optional camera module to take photo of the user if needed for later processing, a processing module to calculate and store user's face representation information, a memory management module to store calculated face representation information, and a communication module to send privacy-preserving messages to nearby devices.

Meanwhile, the device that can take images and/or videos while performing appropriate visual privacy protection processing in such scenario mainly comprises an application module to invoke the camera of the device, a processing module to detect faces from the camera input, calculate face representation information, find matched faces, and do de-identification process, a communication module to receive privacy-preserving messages sent by nearby devices, a display

module to present real-time feedbacks on the screen of the device, and a memory management module to save photo or image after necessary privacy protection actions.

According to an embodiment of the present invention, the visual privacy protection method performs with a wireless communication and a camera module within the smart device. For the device which wants its user's privacy to be protected, the method is composed of the steps of:

calculating face representation information of the user;

generating a visual privacy protection request;

sending face representation information to other devices within range via wireless network;

For the device which will take images, the visual privacy protection service is composed of the steps of:

invoking camera of the device to take images and/or videos;

receiving the visual privacy protection request from devices within range via wireless network;

extracting face representation information from the visual privacy protection request;

storing the face representation information in a database;

detecting all faces in the input data from camera;

calculating face representation information for faces detected in the camera input data;

comparing calculated face representation information with those stored in the database;

designating faces whose face representation information is matched in the acquired camera data;

performing de-identification process on the acquired camera data for each of the faces to be protected;

displaying processed camera data to the screen and outputting processed camera data to other third-party applications.

This invention mainly offers the following advantages. First, the visual privacy protection method of the present invention can maintain both privacy and utility. It preserves privacy of certain individuals while keeping functionality of the camera and as much information as possible in the images and/or videos. Second, it automatically removes identifiable information of certain individuals without additional efforts from the user.

The invention guarantees the privacy of people who are captured by a digital camera of mobile and wearable devices, e.g., smart phone and smart glass. The visual privacy preserving method of the present invention can be provided by the system of devices that guarantees the privacy of people on photos and/or videos taken by mobile and wearable devices.

Brief Description of the Drawings

The accompanying drawings, which are included to provide a further understanding of the present invention and are incorporated in and constitute a part of this application, illustrate embodiment(s) of the present invention, and together with the description serve to explain the principle of the present invention. In the drawings:

Figure 1 shows an ordinary video and/or image capturing scene according to an embodiment of the invention,

Figure **2** shows an embodiment of a user interface of a mobile device according to the invention,

Figure 3 shows a generalized diagram of the system according to an embodiment of the invention,

Figure 4 shows a network according to an embodiment of the invention,

Figure **5** shows the workflow on the transmitter side according to an embodiment of the invention,

Figure 6 shows the workflow on the receiver side according to an embodiment of the invention,

Figure 7 illustrates the operating system structure of a computing system, as an example mobile device operating system according to an embodiment of the invention,

Figure 8 illustrates the operating system structure of an alternative computing system, as a mobile device operating system according to an embodiment of the invention, and

Figure 9 shows the preferred location of the privacy-preserving in a generalized device architecture for most mobile operating systems according to an embodiment of the invention.

Detailed description of the invention

Hereinafter, exemplary embodiments of the present invention will be described in detail with reference to the accompanying drawings. Meanwhile, the configuration of a system and method, which will be described below, are merely given to describe the preferred embodiments of the present invention, and are not intended to limit the scope of the present invention. The same reference numerals used throughout the specification refer to the same constituent elements.

It is noted that for the ease of explanation, the preferred embodiments are explained in terms of single images. However, skilled person recognizes how the present invention can be adapted to video data, i.e. regarding each frame of a video as a series of single images. It is further noted that for the ease of explanation, the majority of the preferred embodiments are explained for a smart phone. However the skilled person recognizes how the present invention can be adapted to other smart wearable devices, e.g., as smart glass that have the wireless communication means. In addition, it is noted that the terms face representation information and abstract facial feature data are used for the purpose of explanation, both terms stand for the same concept and are interchangeable.

Though some illustrative examples are used to describe the details of this invention, it should be realized that the implementations of the invention should not be confined with the limited examples and additional modifications can be applied to adapt the system to more application scenarios.

Figure 1 shows an ordinary video and/or image capturing scene 100 according to an embodiment of the invention, i.e. this diagram illustrates a scene in the real world when a user takes a picture and/or video at a place with a number of people around. In the scene, the photographer A 101 is taking a picture and/or recording a video of the target individual B 103. Target individual B 103 approves photographer 101 to collect his or her visual information. However, in many circumstances, some people who do not be willing to be included in this photograph or video

may be present in the background. The person D 105 represents one who wants his or her face de-identified in the collected visual information. To achieve this, person D 105 can set his or her device (e.g. smart phone) 106 to a mode where the device 106 will send a message notifying all other devices nearby 102, 104, 108 to de-identify the face of the person D 105 once any visual information with the face of the person D 105 is collected. Since person B 103 is the target individual who would like his or her face in the photo or video, B's device 104 will not be set to the same mode which device 106 is currently in. Person C 107 in FIG.l is also a passer-by, but the person CI07 does not mind being recorded by nearby devices. Then, C's device 108 can be in the same mode as B's device 104. The camera module of A's device 102 is currently activated as A is performing visual information collection. Once the camera is activated, A's device 102 will receive all relevant message from nearby devices to determine which faces in the visual file should be de-identified.

The devices in Fig.l, namely devices 102, 104, 106, and 108 do not have to be hand-held devices as shown in the diagram. Wearable devices whose operating systems have privacy-preserving module incorporated can also achieve similar functionality. It is noted that the number of individuals being photographed and/or videotaped do not limited to three. In other words the number of individuals within a particular scene can be any number of individuals. The number of people photographed and/or videotaped in the scene can be any number of individuals smaller or equal to the number of individuals in the scene. A detailed implementation of the system according to the present invention will be demonstrated within subsequent figures.

Figure 2 shows an embodiment of a user interface of a mobile device according to the invention. More specifically Fig. 2 illustrates the example user interface 200 on a screen 202 of a device 201, which is currently taking a photo and/or recording a video. Individuals 203, 209, and 206 can be seen as corresponding to individuals 103, 107, 105, c.f., Fig.l. Individual 206 would not like his or her facial information to be collected and sets his or her device 207 to send a visual privacy protecting requests to all nearby devices 201, 204, 210. Device 201 receives the request from device 207 and it is mandatory for device 201 to satisfy this request and blur, i.e., de-identify, face 208 of individual 206, as is shown on the screen 202. Devices 204, 210 of individuals 203 and 209 respectively, do not need to receive the request from device 207, since their camera modules are not activated. Both individual 203 and 209 are not sending any visual

privacy protecting request because the respective individuals approve visual information collection on this occasion. Hence, device 201 will not process the visual information of 203 and 209, and faces 211 and 205 will be shown as normal on the screen 202.

Figure 3 shows a generalized diagram of the system according to an embodiment of the invention. The visual privacy-preserving system 300 is generalized into six modules. Application module 301preferably comprises a system camera application and a third party camera application, with both of which the user may directly interact with. Both types of applications will invoke the camera module 302. The camera module 302 mainly refers to the camera driver in the kernel layer and the underlying camera hardware for collection of optical information. The processing module 304 primarily encompasses the face detection process, facial feature data extraction, and image de-identification processes. The communication module 303 is responsible for device-to-device message transmission and reception. The display module 305 offers real-time visual feedbacks to the photographer on what the saved image and/or video file will look like. Memory management module 306 takes effect when saving a photo and/or video into the device memory and is further responsible for storing the received abstract facial feature data.

Figure 4 shows a network according to an embodiment of the invention. In the network 400 four devices 401, 402, 403, and 404 are connected to each other. Devices 401, 402, 403, and 404 are all in different states. Device 401 is in the privacy-preserving mode and the camera module of 401 is activated. Device 402 is not in the privacy-preserving mode and the camera module is activated. Device 403 is in the privacy-preserving mode but the camera is not activated. Device 404 is not in the privacy-preserving mode and the camera is not activated. It should be noted that one device can be transmitting and receiving privacy-preserving messages at the same time. Devices in the privacy-preserving mode , i.e., devices 401 and 403, will send request messages to all other devices nearby, but only those devices whose camera is on, i.e., devices 401 and 402, will receive the message. In other words, the reception of this message is camera-associative.

The message transmission mechanism is in a device-to-device fashion, although the exact transmission protocol this privacy-preserving system follows should not be limited to one particular type. Wi-Fi, Bluetooth etc. are all likely to be considered as appropriate according to different application scenarios. Reference numerals 405, 406, and 407 represent respective message sent by device 401 and device 403. These messages each comprises of two categories of

data: identification data and feature data. Feature data is used to determine which person in the photo or video requests face de-identification. Identification data helps the receiver identify that the received message is related to privacy-preserving request. Detailed procedures of this privacy-preserving system are elucidated in two flow charts in Fig.5 and Fig.6.

Figure 5 shows the workflow 500 on the transmitter side, which are the devices sending visual privacy protection requests to other devices. When a user sets his or her device to the privacy-preserving mode, i.e., when individual 105 sets the device 106 to send the visual privacy protection requests for the first time, decision stage 501 is reached. The operating system will determine whether the device has previously been in the privacy-preserving mode and whether previous feature data exists. If not, or if the user chooses to renew the feature data, in stage 502, the device will ask the user to input a facial photo.

This process may evoke the camera module of the device depending on whether the user chooses to take a new photo as input or use an old photo. The photo input preferably includes no other person's face apart from the user's, and the face of the user is preferably in a frontal pose. This has the advantage, that the subsequent processes become more easy and accurate with respect to limitations on further face detection and recognition methods.

The data 402 is the output data of process 401, a facial image file, possibly in but not limited to the JPEG format. After a facial image is fed in, in stage 504, face detection process initiates and locates the face regions, producing output 505. Then, in stage 506, the standard feature extraction process is executed. This feature extraction method is preferably based on one of many high-performance face recognition algorithms known to the skilled person. For instance, a non-statistical face recognition method, e.g., Local Gabor Binary Pattern Histogram Sequence (LGBPS), is suitable for this application scenario, since it does not rely on a large number of samples and its performance has also been proved qualified.

It should be noted that the applied feature extraction method is not limiting the scope of the invention and any applicable method can be used to carry out the invention. However, once an optimal face recognition mechanism is chosen, it is preferably be made to be the standard across different devices, in order to ensure the following comparison process to be valid.

From process 506 the data 507, abstract feature data of the user's face, will be output and saved to the device memory for future purposes in stage 510. After combining feature data with the identification data as explained with reference to Fig.4, the device will preferably constantly send the combined data to all nearby devices in stage 50 until the privacy-preserving mode is turned off.

Figure 5 can be divided into several blocks according to the module generalization illustrated in Fig.3. Block 511 is related to the camera module since a new photo may be taken in image collection process. Block 512 belongs to the process module where image outputs from the camera module are processed. Block 513 pertains to the communication module where privacy protection requests are transmitted. Block 514 is part of the memory management module. Memory management module and display module also participate in several other processes shown in Fig. 5.

Figure 6 shows the workflow 600 on the receiver side according to an embodiment of the invention. In decision stage 601, once a camera-based application is started, whether or not it originates from the operating system or a third-party, the device is forced to execute process 603. The device will receive all relevant privacy-preserving request messages.

Since multiple users may be sending requests in the same time, the device is likely to receive multiple request messages, resulting in a received feature data pool 605. Each discrete element in this data pool represents the abstract facial information of one user who is not willing to be photographed or videotaped. In the meantime, before the real-time frames are passed from the camera module to the display module and can be saved as a visual file in memory management module, some transitional steps will be performed first in the process module.

In process 602, the image data from the camera hardware will be passed to the face detection process to locate regions of all the existing faces of this frame. Consequently, data 604, a pool of face regions, will be the output of process 602. Subsequently, in stage 606, a standard feature extraction process will be carried out. The feature extraction is preferably standardized across all devices with the same operating system. The feature extraction is preferably performed separately on different face regions, thus producing another abstract feature data pool 607.

In stage 608, comparison process will be performed on the received feature pool from the communication module and that from the camera module in a pairwise fashion. In decision stage 608 a corresponding face region in the frame will be passed to process 609 to be de-identified, once a piece from pool 607 matches with a piece from pool 605. De-identification can be achieved in multiple ways. For example, simply blurring the face or substituting the face with a randomly generated face. If a piece from pool 604 has no match in pool 605, the corresponding face region will not be processed.

After a match, i.e., the piece from pool 604 is found in pool 605, the comparison process for the next piece in pool 604 is carried out. Until in stage 611, the system makes sure all pieces from 604 have been compared. Then, this frame of visual information can be passed to the display module and updates what the photographer can see on the screen. Also, all the photo and video files saved to the device memory are not the direct output from the camera hardware but the de-identified data as it has been passed to the device display. In stage 612, after the camera application ends, all the received feature data is preferably deleted from the device.

In terms of the generalized modules shown in Fig.6, block 620 belongs to the camera module. The following block 640 which refers the communication module and is part of the memory management module where received facial feature data is stored, and block 630 which is part of the process module will only initiate execution if the camera module is active. Block 650 is also affiliated to the process module, while block 660 is associated with the memory module.

During the entire process, the display module actively updates the screen of the device. The memory management module also plays a part when the user saves the processed photo and/or video files and received feature data.

Figure 7 illustrates the operating system structure 700 of a computing system, as an example mobile device operating system according to an embodiment of the invention. Block 710, the kernel, is the base of the entire software stack and primarily manages the device hardware and also offers several additional functionalities. Just above block 710 is block 720, including the hardware abstraction layer, the core libraries and several other components. The hardware abstraction layer permits the applications in the topmost level to employ the hardware in the bottommost level through a simple application programming interface. Block 730 includes, e.g., a Dalvik virtual machine, which interprets the bytecode of applications for the device runtime

environment. Block 740 encompasses various system services, for example, power manager, sensor service etc. The layer 750 on the top is the application layer which users can directly interact with.

Figure 8 illustrates the operating system structure 800 of an alternative computing system, as a mobile device operating system according to an embodiment of the invention. The basic framework of the system is similar to 700 with slight nuances. Layer 810 the core OS layer is responsible for device management and memory management layer as 710. Layer 820 core services layer incorporates system libraries and an Objective-C runtime environment. Layer 830 the media layer contains the graphics, audio, and video technologies utilized to develop multimedia applications. Layer 840 refers to the cocoa touch layer which contains key frameworks for application development and provides many high-level system services. As layer 750, layer 850 is the application layer.

Figure 9 shows the preferred location of the privacy-preserving in a generalized device architecture for most mobile operating systems according to an embodiment of the invention. Hardware layer 910 serves as the most fundamental component of the entire architecture. Kernel layer 920 together with libraries and hardware abstraction layer 930 manage the accessibility of hardware for high-level software. Camera applications belong to the topmost level 950, the application layer. In between, layer 940, the system services layer offers many high-level frameworks for application developers. Since system services layer is accessible to developers, to ensure the validity of the privacy protection service, the service 960 should be implemented below the system services layer. Layer 920 and 930, however, are not prone to malicious manipulations. Hence, privacy protection service 960 may be parallel or even overlapping with layer 930.

While the present invention has been described in connection with certain preferred embodiments, it is to be understood that the subject-matter encompassed by the present invention is not limited to those specific embodiments. On the contrary, it is intended to include any alternatives and modifications within the scope of the appended claims.

Claims

1. A method for visual privacy protection of individuals in a network with at least one first mobile device and at least one second mobile device, the mobile devices having at least one camera, the mobile devices being connected to each other within the network and/or having a direct wireless connection and the method comprising the steps of:

A) the second mobile device receiving at least one visual privacy protection request from the first mobile device,

B) the second mobile device processing the information contained in the at least one visual privacy request using a second database on the second mobile device;

C) the second mobile device processing acquired camera data using the information contained in the second database;

D) the second mobile device providing processed acquired camera data to a screen and/or outputting the processed acquired camera data to at least one application preferably running on the second mobile device.

2. The method of claim 1, wherein the visual privacy request comprises face representation information of an individual to be protected.

3. The method of claim 1 or 2, wherein prior to the step A) the first mobile device performs the step of generating the at least one visual privacy protection request preferably further comprising the steps of

Al) the first mobile device calculating a face representation information from a facial picture of an individual to be protected, if no previous face representation information for the individual to be protected exists in a first database of the first mobile device;

A2) the first mobile device generating a visual privacy protection request containing the face representation information of the individual to be protected and preferably further information to be sent; and/or

A3) the first mobile device further performs the step of sending the visual privacy protection request to all other devices in the network and/or in range of the direct wireless connection preferably in a predetermined time interval.

4. The method of any one of claims 1 to 3, wherein the step B) of processing the information contained in the at least one visual privacy request further comprises the steps of:

Bl) the second mobile device extracting the face representation information from the visual privacy request;

B2) the second mobile device storing face representation information in the second database in the second mobile device; and

B3) the second mobile device updating the database, if

a) a new face representation information has been extracted storing the respective face representation information, or

b) a visual privacy request has been expired, wherein

preferably determining the expiration of a visual privacy request is based on a judgment whether the second mobile device does not receive the respective visual privacy again within a predetermined period of time, as

i) the first mobile device does not send the respective visual privacy request anymore, or

ii) the first mobile device is no longer in the same network and/or in the range of the direct wireless connection.

5. The method of any one of claims 1 to 4, wherein the step C) of processing acquired camera data using the information contained in the at least one visual privacy request further comprises the steps of:

CI) the second mobile device detecting all faces in the acquired camera data from the at least one camera;

C2) the second mobile device calculating a face representation information for each of all faces detected in the acquired camera data;

C3) the second mobile device comparing each of the calculated face representation information with the face representation information stored in the second database preferably in a pair wise fashion;

C4) the second mobile device designating each face as a face to be protected if a match is found; and

C5) the second mobile device performing a de-identification process on the acquired camera data taking into account each of the faces to be protected.

6. The method of claim 5, wherein the de-identification process of step C5) comprises at least one of the following steps:

a) altering the data of the camera input data in the region of each of the faces to be protected;

b) altering the data of the camera input data in the region of at least one of the faces to be protected by blurring the face to be protected ;

c) altering the data of the camera input data in the region of at least one of the faces to be protected by substituting the face with default data, preferably the default data being a randomly generated face; and

d) deleting the data of the camera input data in the region of at least one of the faces to be protected.

7. A first mobile device being configured to perform the steps of the method according to claim 3.

8. A second mobile device being configured to perform at least one of the steps of the method according to any one of claims 1 to 6.

9. A system for visual privacy protection of individuals for mobile devices, the system comprising at least one first mobile device according to claim 7 and at least one second mobile device according to claim 8.

10. The system of claim 9, wherein each mobile device has a privacy-preserving module and at least one of the following: a display module; a camera module; a memory management module; and a communication module.

11. The system of claim 10, wherein the respective privacy-preserving module is configured to perform at least one of the steps of any one of claims 1 to 6; wherein

the privacy-preserving module preferably being located in a layer close to the operating system; and/or

the privacy-preserving module preferably being not accessible by any third-party applications or developers; and/or

the privacy-preserving module preferably being below a system services layer, preferably parallel and/or overlapping with a libraries layer.

Figures

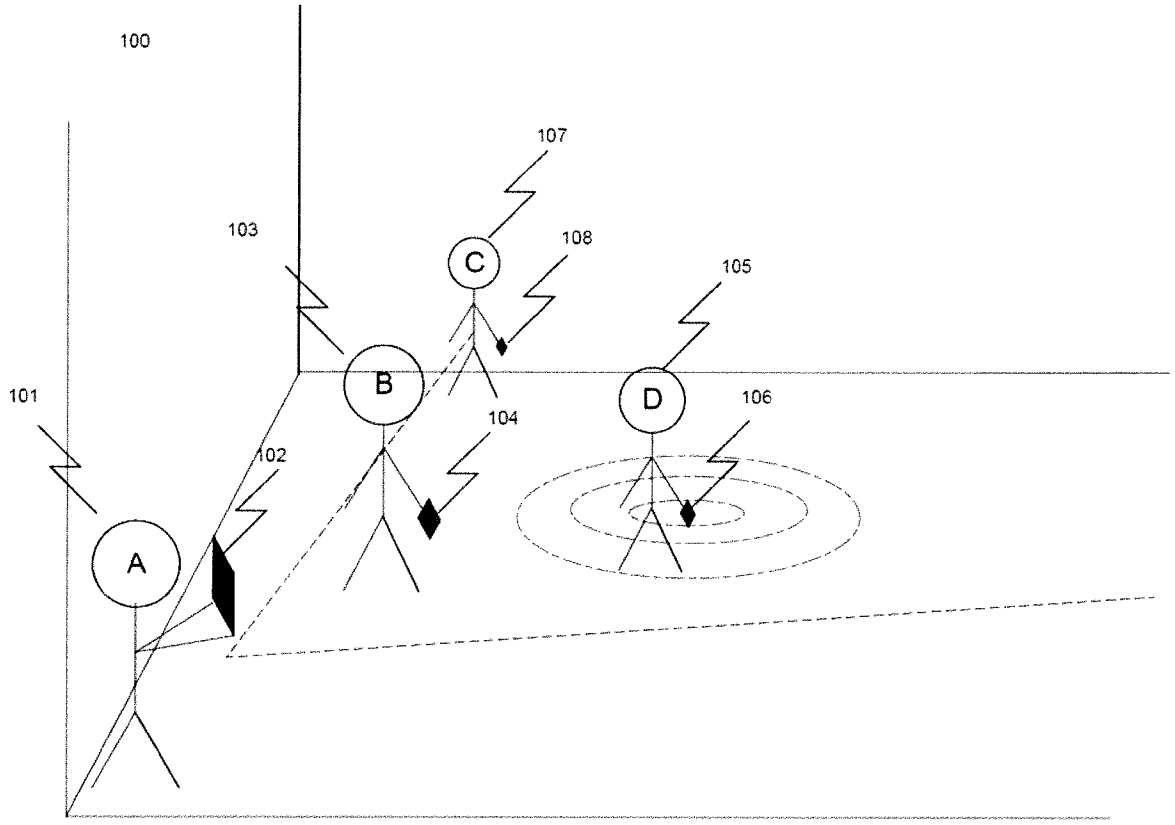

Figure 1

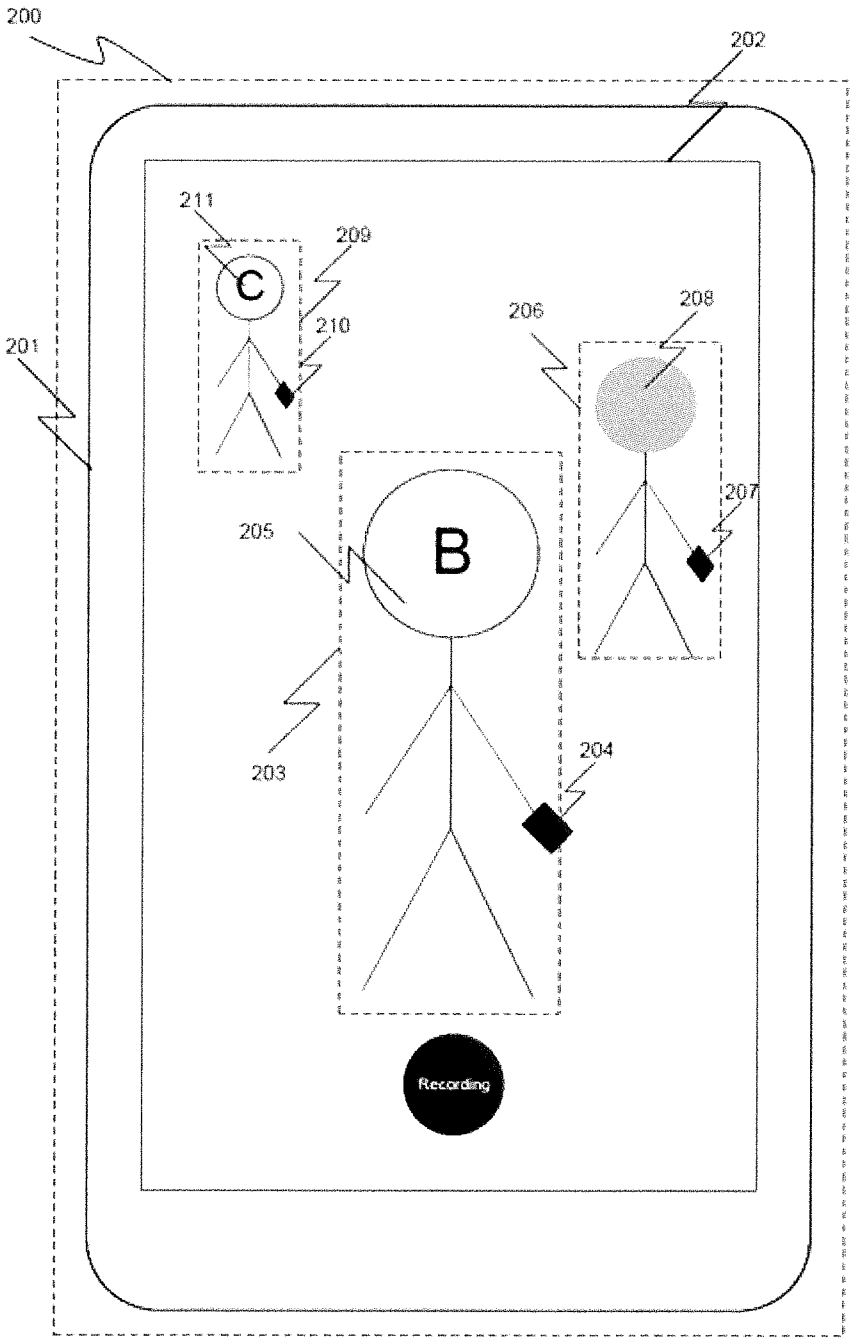

Figure 2

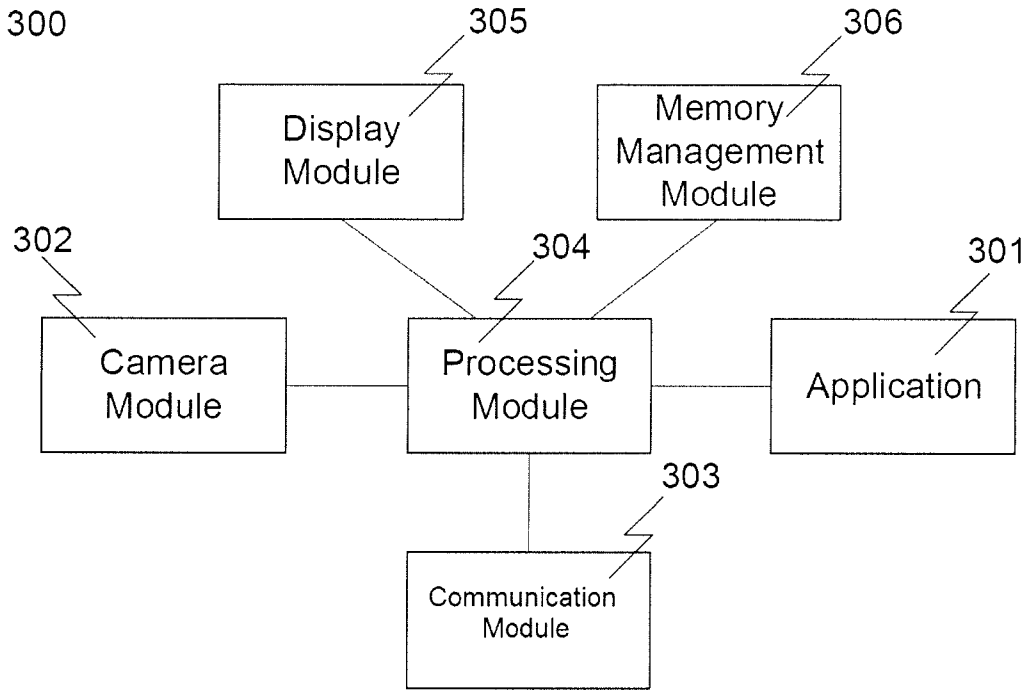
300
305
306
Display Module
Memory Management Module
302
304
301
Camera Module
Processing Module
Application
303
Communication Module

Figure 3

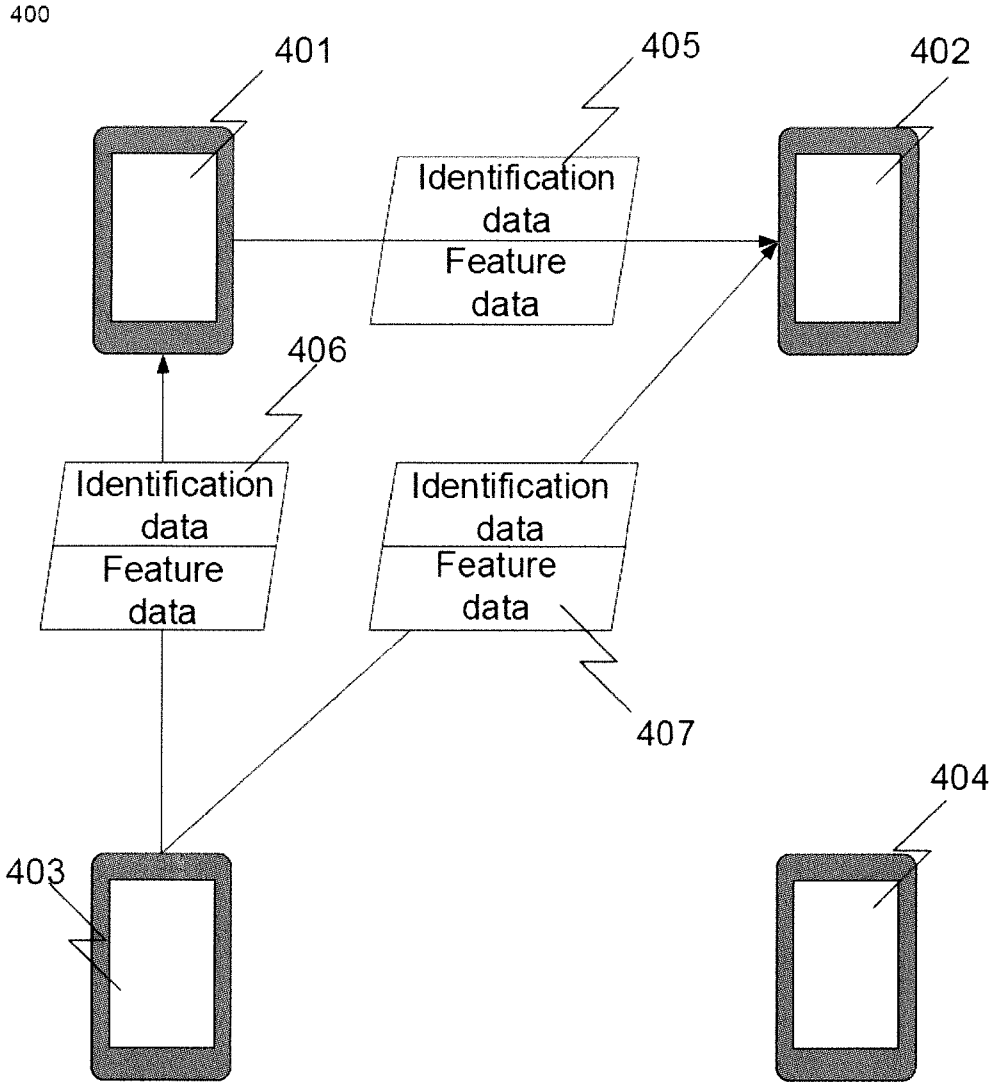
400
401
405
402
Identification data
Feature data
406
Identification data
Feature data
Identification data
Feature data
407
404
403

Figure 4

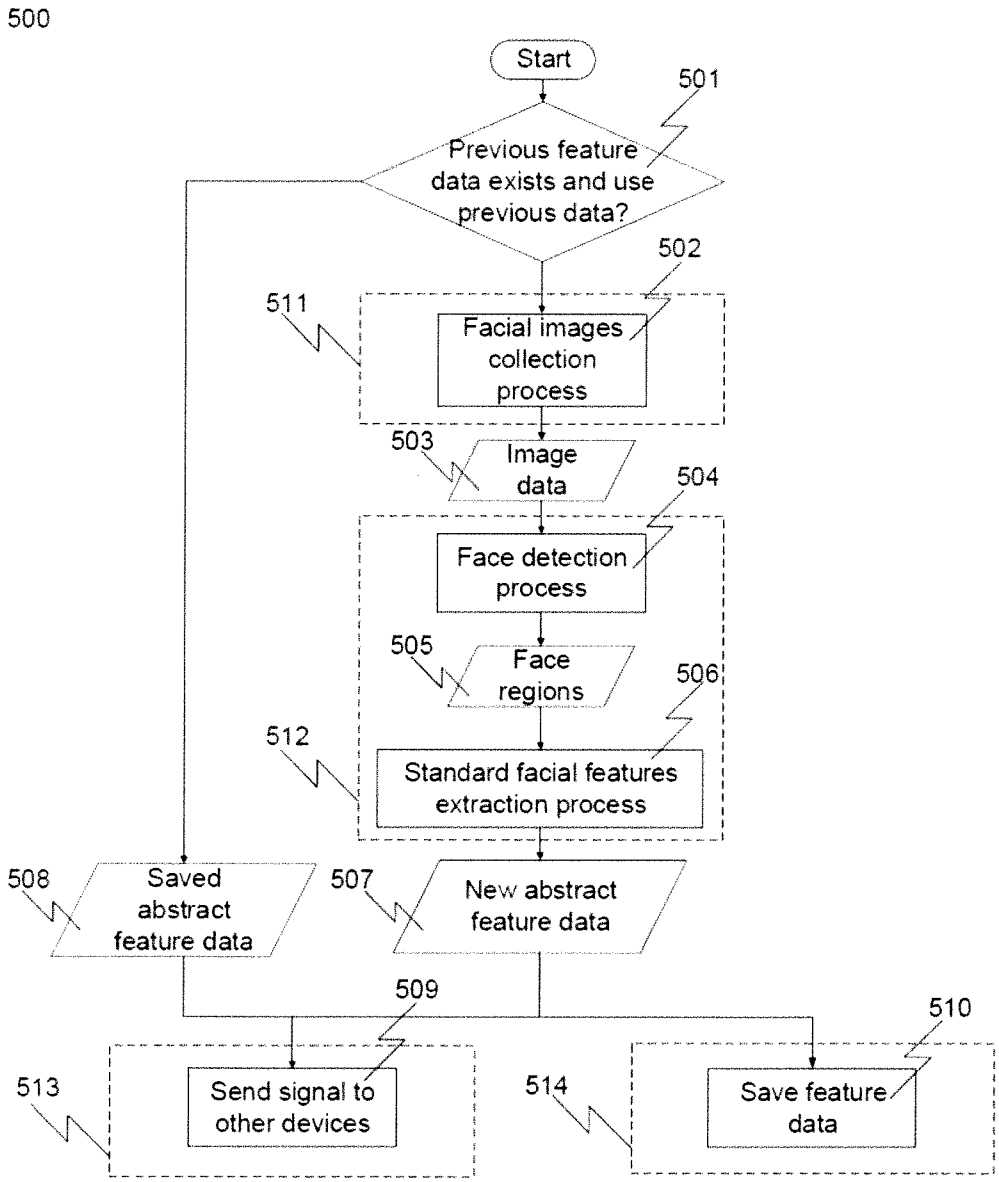
500
Start
501
Previous feature data exists and use previous data?
502
511
Facial images collection process
503
Image data
504
Face detection process
505
Face regions
506
512
Standard facial features extraction process
508
Saved abstract feature data
507
New abstract feature data
509
510
513
Send signal to other devices
514
Save feature data

Figure 5

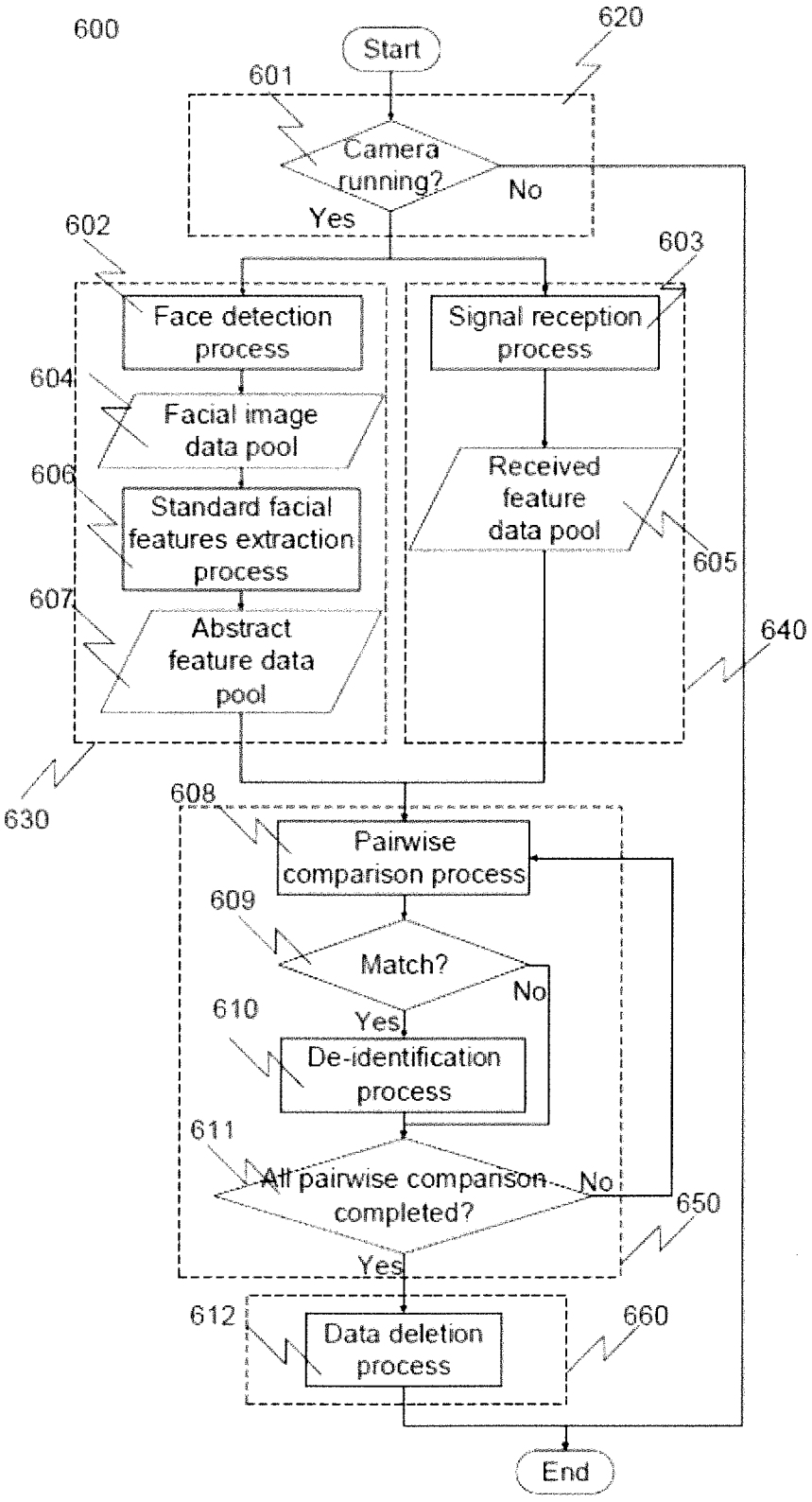
600
Start
620
601
Camera running?
No
Yes
602
603
Face detection process
Signal reception process
604
Facial image data pool
606
Standard facial features extraction process
Received feature data pool
605
607
Abstract feature data pool
640
630
608
Pairwise comparison process
609
Match?
No
Yes
610
De-identification process
611
All pairwise comparison completed?
No
650
Yes
612
Data deletion process
660
End

Figure 6

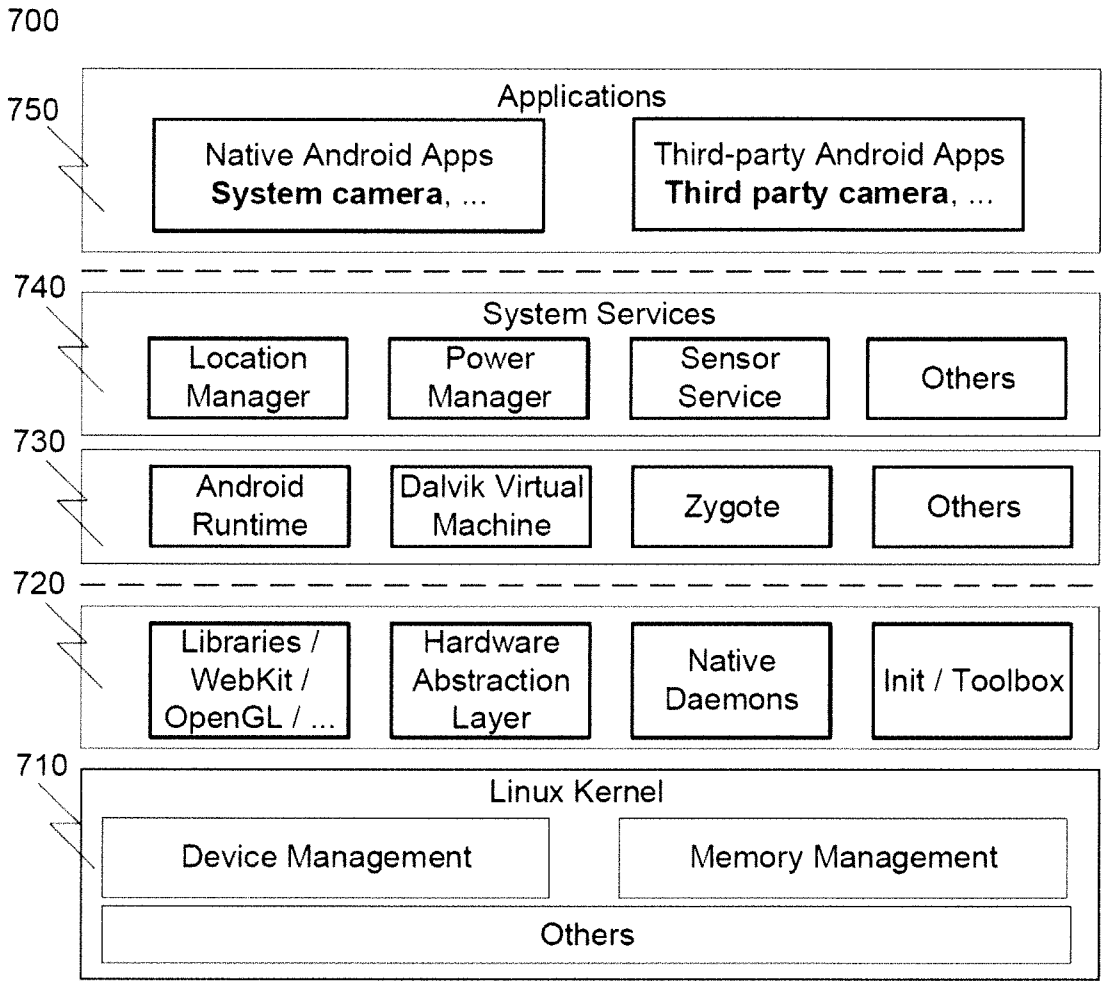
700
750
Applications
Native Android Apps
System camera, ...
Third-party Android Apps
Third party camera, ...
740
System Services
Location Manager
Power Manager
Sensor Service
Others
730
Android Runtime
Dalvik Virtual Machine
Zygote
Others
720
Libraries / WebKit / OpenGL / ...
Hardware Abstraction Layer
Native Daemons
Init / Toolbox
710
Linux Kernel
Device Management
Memory Management
Others

Figure 7

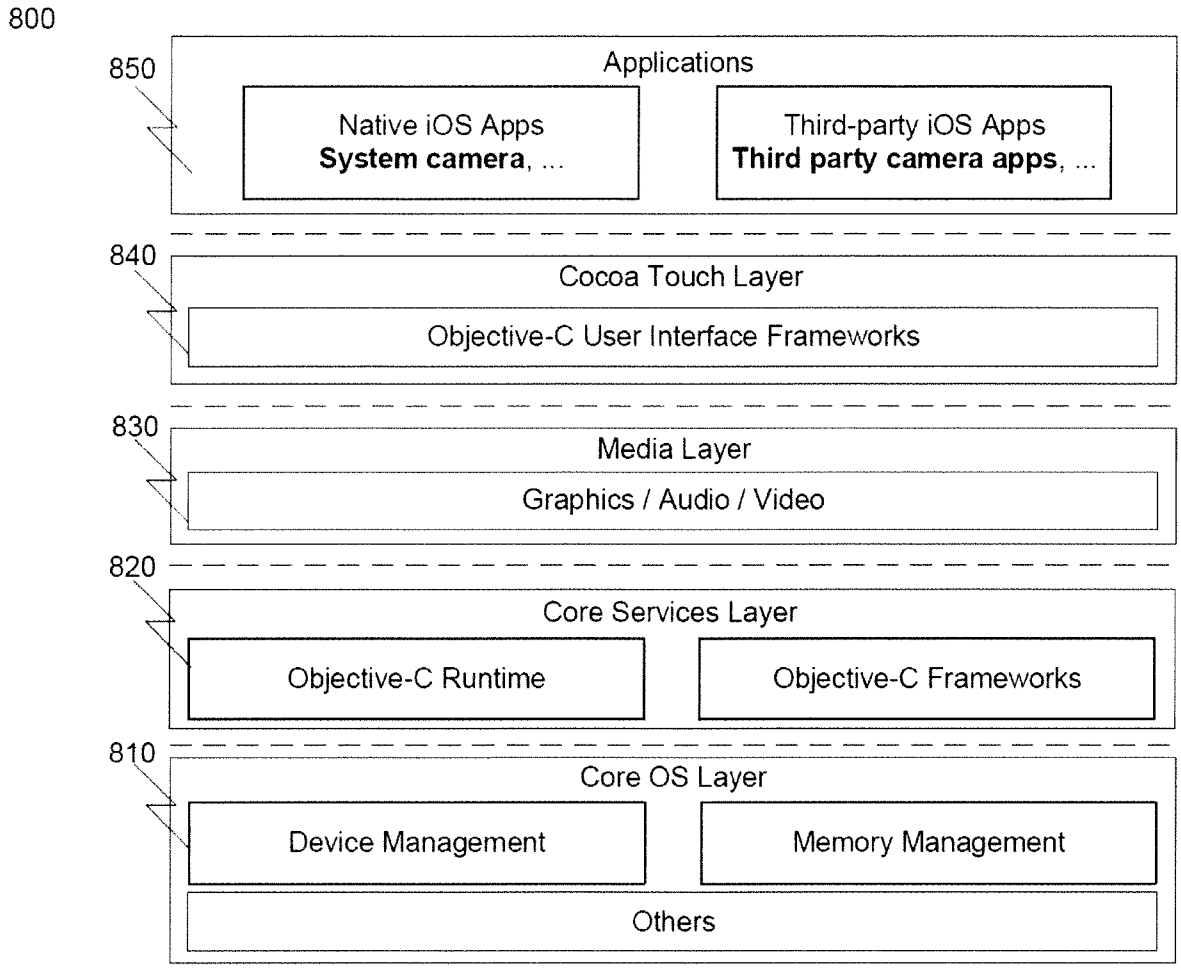
800
850
Applications
Native iOS Apps
System camera, ...
Third-party iOS Apps
Third party camera apps, ...
840
Cocoa Touch Layer
Objective-C User Interface Frameworks
830
Media Layer
Graphics / Audio / Video
820
Core Services Layer
Objective-C Runtime
Objective-C Frameworks
810
Core OS Layer
Device Management
Memory Management
Others

Figure 8

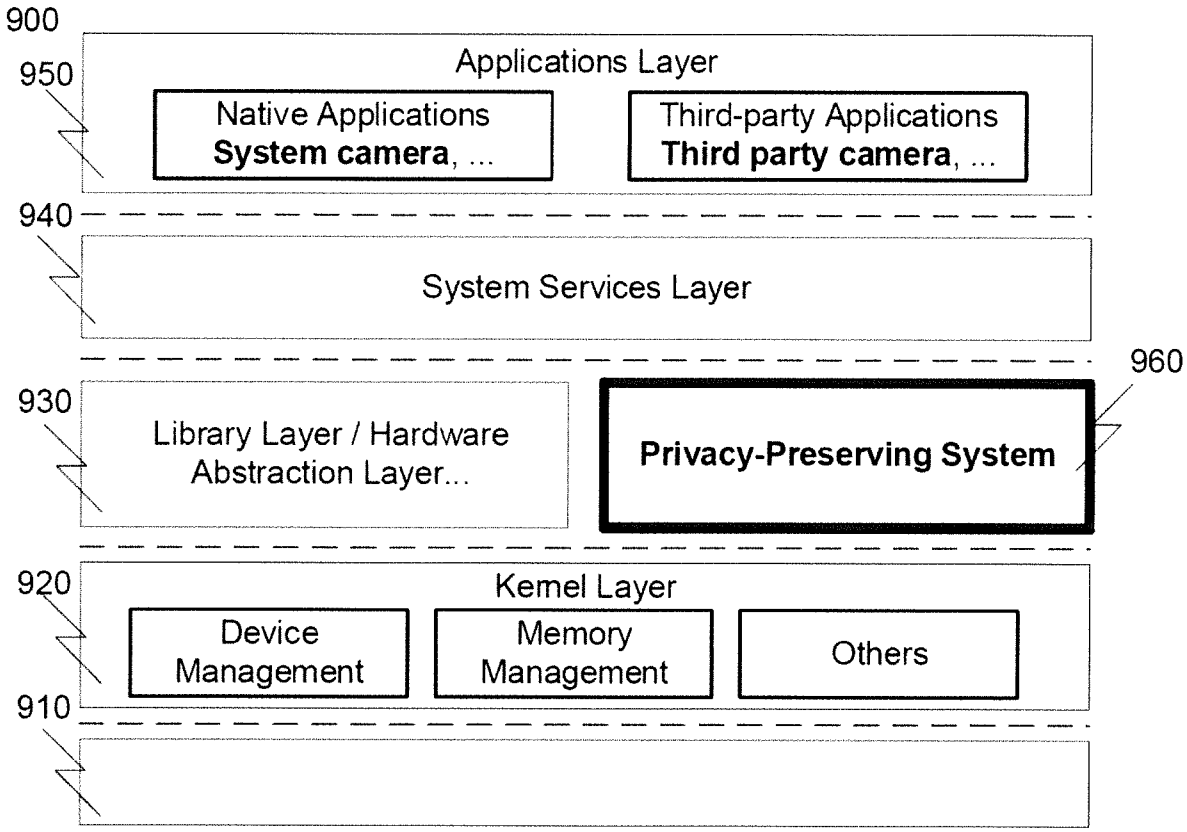
900
950
Applications Layer
Native Applications
System camera, ...
Third-party Applications
Third party camera, ...
940
System Services Layer
960
930
Library Layer / Hardware
Abstraction Layer...
Privacy-Preserving System
920
Kernel Layer
Device
Management
Memory
Management
Others
910

Figure 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/055726

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/62
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

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.
Y	WO 2014/028009 A1 (EMPIRE TECHNOLOGY DEV LLC [US]; UR SHMUEL [IL]; MARGALIT MORDEHAI [IL]) 20 February 2014 (2014-02-20) paragraph [0013] - paragraph [0018]; figure 1 paragraph [0020] - paragraph [0021] paragraph [0025] - paragraph [0042]; figure 2 paragraph [0055] - paragraph [0060]; figure 5	1-11
Y	GB 2 400 514 A (HEWLETT PACKARD DEVELOPMENT CO [US]) 13 October 2004 (2004-10-13) page 13, line 22 - page 14, line 12; figure 9	1-11

-/-

[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" documentwhich may throw doubts on priority claim(s) orwhich 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
30 November 2016	07/12/2016

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	Vinck, Bart

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/055726

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 388 802 A2 (OMRON TATEISI ELECTRONICS CO [JP]) 11 February 2004 (2004-02-11) paragraph [0028] ; figure 2 paragraph [0029] ; figure 3 paragraph [0030] ; figure 4	1-11
A	US 2011/202968 Al (NURMI MI KK0 [FI]) 18 August 2011 (2011-08-18) paragraph [0030]	1-11

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2016/055726

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2014028009 A1	20-02-2014	KR 20150045477 A	28-04-2015
		US 2014196152 A1	10-07-2014
		US 2016171244 A1	16-06-2016
		WO 2014028009 A1	20-02-2014
GB 2400514 A	13-10-2004	GB 2400514 A	13-10-2004
		US 2004202382 A1	14-10-2004
EP 1388802 A2	11-02-2004	AT 394751 T	15-05-2008
		CN 1472691 A	04-02-2004
		EP 1388802 A2	11-02-2004
		JP 4036051 B2	23-01-2008
		JP 2004062560 A	26-02-2004
		US 2004081338 A1	29-04-2004
US 2011202968 A1	18-08-2011	NONE	