Title: BACKGROUND ENROLLMENT AND AUTHENTICATION OF A USER

Abstract: An electronic device can include a processing device operatively connected to a biometric sensing device. The biometric sensing device may capture a biometric image each time a user interacts with the electronic device. When the user enters user identification data (UID) and a biometric image was recently captured, the biometric image is tagged with the UID. The user can access the electronic device and/or an application being accessed on the electronic device when a subsequently captured biometric image matches a tagged biometric image or an untagged biometric image that is assigned to a cluster that includes a tagged biometric image.
Published:

— with international search report (Art. 21(3))
BACKGROUND ENROLLMENT AND AUTHENTICATION OF A USER

Cross-Reference to Related Application

[0001] This Patent Cooperation Treaty patent application claims priority to U.S. non-provisional application No. 14/022,110, filed September 9, 2013, and titled "Background Enrollment and Authentication of a User", the contents of which are incorporated herein by reference in their entirety.

Technical Field

[0002] The present invention relates to electronic devices, and more particularly to a biometric sensing device included in, or connected to an electronic device.

Background

[0003] Biometric devices are increasingly common in computer or network security applications, financial applications, and surveillance applications. Biometric devices detect or image a unique physical or behavioral trait of a person, providing biometric data that can reliably identify the person. For example, a fingerprint includes a unique pattern of ridges and valleys that can be imaged by a fingerprint sensor. The image of the fingerprint, or the unique characteristics of the fingerprint, is compared to previously captured reference data, such as a reference fingerprint image. The identity of the person is obtained or verified when the newly captured fingerprint image matches the reference fingerprint image.

[0004] Typically, a user has to enroll reference biometric data that will be used for authentication. For example, a user may have to enroll one or more fingerprints before he or she can use the fingerprints for authentication. During the enrollment process, an image of each fingerprint that will be used for authentication is acquired and extracted features of the fingerprint are stored in a memory. The extracted features can then be used as reference fingerprint data during the authentication process. In some situations, however, the user may have to scan a fingerprint a number of times to obtain a fingerprint image that has adequate fingerprint coverage and an acceptable resolution. For example, a user may move or shift the finger during image capture, which can produce a blurry fingerprint image. Alternatively, contaminants such as dirt and water may be present on the finger being scanned, which can adversely affect the fingerprint image and/or the ability of the fingerprint sensor to obtain a
fingerprint image. These and other challenges can be exacerbated when a user has to enroll multiple fingerprints.

[0005] Even after enrolling the biometric data and using a biometric sensing device to authenticate the identity of a user, a user may still be required to enter a password or pin when the user wants to access an application, a website, or another device. Thus, a user may be required to repeatedly enter pins or passwords when the user launches or switches applications, functions, and websites.

Summary

[0006] Embodiments described herein acquire biometric images in the background as a user interacts naturally with an electronic device. Authentication of the user can also be done in the background using a newly captured biometric image and a previously captured biometric data that is tagged with user identification data (UID) such as a password or pin. A biometric sensing device can be operatively connected to a processing device in an electronic device, such as a processing device in a laptop computer, a tablet computing device, and a smart telephone. In some embodiments, the biometric sensing device can be positioned at a location that a user’s physical or behavioral trait is naturally detectable, in contact with, or in close proximity to as the user interacts with the electronic device. A method for authenticating a user can include capturing at a first time a first biometric image when the user interacts with the electronic device and tagging the first biometric image with a UID that is associated with the user. The UID can be a pin or a password that the user entered within a given time period around the time the first biometric image is captured. Subsequently, a second biometric image can be captured and a determination made as to whether the second biometric image matches the first biometric image tagged with the first UID. The user can be given access to the electronic device and/or to an application being accessed on the electronic device when the second biometric image matches the tagged first biometric image. The application can be an application, a website, an account, and the like that requires the user to enter the UID for access.

[0007] In another aspect, a method for authenticating multiple users of an electronic device that includes a biometric sensing device can include capturing a first biometric image when a first user interacts with the electronic device and tagging the first biometric image with a first UID that is associated with the first user. The first biometric image tagged with the first UID can be assigned to a cluster associated with the first user. Each cluster associated with the first user
can be associated with a respective biometric attribute of the user. For example, when the biometric sensing device is a fingerprint sensor, each cluster associated with the first user can correspond to a respective finger of the first user. A second biometric image can be captured when the first user again interacts with the electronic device. The first user can be given access to the electronic device or to an application being accessed on the electronic device when the second biometric image matches the first biometric image tagged with the first UID. The authentication process is similar for a second user, except that a biometric image is tagged with a UID associated with the second user, and the tagged biometric image can be assigned to a cluster associated with the second user.

[0008] In some embodiments, the biometric images can be fingerprint images. The fingerprint images can be captured when a finger or fingers of the user are in close proximity to, or in contact with an input region of the fingerprint sensor. The fingerprint sensor can be positioned at a location on the electronic device that a user's finger, fingers, and/or hand is naturally in contact with as the user interacts with the electronic device.

[0009] In yet another aspect, an electronic device can include a processing device operatively connected to a biometric sensing device. The biometric sensing device can be configured to capture biometric images when a user interacts with the electronic device. The processing device can be configured to receive each biometric image and tag at least one biometric image with a user identification data (UID) that is associated with the user. The processing device can be configured to determine if a newly captured biometric image matches at least one biometric image tagged with the UID, and if a match exists, provide access to the user to the electronic device and/or an application being accessed on the electronic device.

**Brief Description of the Drawings**

[0010] Embodiments of the invention are better understood with reference to the following drawings. The elements of the drawings are not necessarily to scale relative to each other. Identical reference numerals have been used, where possible, to designate identical features that are common to the figures.

[0011] **FIG. 1** is a perspective view of an example electronic device that can include, or be connected to a biometric sensing device;

[0012] **FIG. 2** is an illustrative block diagram of the electronic device 100 shown in **FIG. 1**;
FIG. 3 depicts an enlarged and simplified cross-section view of a portion of a fingerprint sensor taken along line 3-3 in FIG. 1;

FIG. 4 is a flowchart of a method capturing fingerprint images;

FIG. 5 is a flowchart of a method for associating a fingerprint image captured in the background with a user;

FIG. 6 illustrates one method for assigning fingerprint images to a cluster;

FIG. 7 is a flowchart of a method for authenticating a user using a previously captured and tagged fingerprint image;

FIGS. 8-9 depict methods for combining fingerprint images or UIDs in different clusters; and

FIG. 10 is a flowchart of a method for deleting fingerprint images.

Detailed Description

Embodiments described herein acquire biometric images in the background as a user interacts naturally with an electronic device. Authentication of the user can also be done in the background using a newly captured biometric image and a previously captured biometric image that is tagged with user identification data (UID) such as a password or pin. Thus, in some embodiments, the user does not have to undergo an explicit enrollment process. The biometric sensing device incrementally captures biometric images and groups the images into clusters. As one example, when the biometric sensing device is a fingerprint sensor, the fingerprint images in a cluster can all correspond to the same finger.

In some embodiments, a biometric image captured within a given time period around the time when a user enters a pin, password, or some other user identification data (UID) can be tagged with the UID. Newly captured biometric images can be compared to the biometric images in each cluster to determine if the newly captured biometric image matches at least one biometric image in a cluster. If the newly captured biometric image matches a previously captured biometric image, and the previously captured biometric image is tagged with a UID that is associated with the user, the identity of the user is authenticated and the user can be
provided access to the electronic device or to an application being accessed on the electronic device.

[0022] Any suitable type of biometric sensing device can be included in, or connected to an electronic device. A person’s fingerprint, eye, DNA, vein patterns, typing speed or patterns, gait, voice, face, and heart or brain signals are examples of a physical characteristic or a behavioral trait that can be detected or imaged by a biometric sensing device. A biometric sensing device can employ capacitance, ultrasonic, optical, resistive, thermal, or other sensing technologies to detect or image a biometric attribute. The term "biometric attribute" is meant to encompass a physical or behavioral trait that can be detected by a biometric sensing device.

[0023] As used herein, the terms “image” and “biometric image” includes an image and other types of data that can be captured by a biometric sensing device. The term "fingerprint image" includes an image and other types of data that can be captured by a fingerprint sensor. By way of example only, a fingerprint sensor can produce a data structure that defines the features in a fingerprint. Additionally, the term "fingerprint image" is meant to encompass an image or other data relating to a fingerprint of some or all of one or more fingers, some or all of a palm, some or all of a hand, and various combinations thereof. The term “finger” is meant to encompass one or more fingers, some or all of a palm, some or all of a hand, and various combinations thereof.

[0024] Directional terminology, such as "top", "bottom", "front", "back", "leading", "trailing", etc., is used with reference to the orientation of the Figure(s) being described. Because components of embodiments described herein can be positioned in a number of different orientations, the directional terminology is used for purposes of illustration only and is in no way limiting. When used in conjunction with layers of a display or device, the directional terminology is intended to be construed broadly, and therefore should not be interpreted to preclude the presence of one or more intervening layers or other intervening features or elements. Thus, a given layer that is described as being formed, positioned, disposed on or over another layer, or that is described as being formed, positioned, disposed below or under another layer may be separated from the latter layer by one or more additional layers or elements.

[0025] Referring now to FIG. 1, there is shown a perspective view of one example of an electronic device that can include, or be connected to a biometric sensing device. In the illustrated embodiment, the electronic device 100 is implemented as a smart telephone. Other embodiments can implement the electronic device differently, such as, for example, as a laptop.
or desktop computer, a tablet computing device, a gaming device, a wearable computing device or display, a display, a digital music player, and other types of electronic devices that include, or be connected to a biometric sensing device.

[0026] The electronic device 100 includes an enclosure 102 at least partially surrounding a display 104 and one or more buttons 106 or input devices. The enclosure 102 can form an outer surface or partial outer surface and protective case for the internal components of the electronic device 100, and may at least partially surround the display 104. The enclosure 102 can be formed of one or more components operably connected together, such as a front piece and a back piece. Alternatively, the enclosure 102 can be formed of a single piece operably connected to the display 104.

[0027] The display 104 can be implemented with any suitable technology, including, but not limited to, a multi-touch sensing touchscreen that uses liquid crystal display (LCD) technology, light emitting diode (LED) technology, organic light-emitting display (OLED) technology, organic electroluminescence (OEL) technology, or another type of display technology. The button 106 can take the form of a home button, which may be a mechanical button, a soft button (e.g., a button that does not physically move but still accepts inputs), an icon or image on a display or on an input region, and so on. Further, in some embodiments, the button 106 can be integrated as part of a cover glass of the electronic device.

[0028] FIG. 2 is an illustrative block diagram of the electronic device 100 shown in FIG. 1. The electronic device 100 can include the display 104, a processing device 200, memory 202, an input/output (I/O) device 204, a sensor 206, a power source 208, a network communications interface 210, and a biometric sensing device 212. The display 104 may provide an image or video output for the electronic device 100. The display may also provide an input surface for one or more input devices, such as, for example, a touch sensing device and/or a fingerprint sensor. The display 104 may be substantially any size and may be positioned substantially anywhere on the electronic device 104.

[0029] The processing device 200 can control some or all of the operations of the electronic device 100. The processing device 200 can communicate, either directly or indirectly, with substantially all of the components of the electronic device 100. For example, a system bus or signal line 214 or other communication mechanisms can provide communication between the processing device 200, the memory 202, the I/O device 204, the sensor 206, the power source
208, the network communications interface 210, and/or the biometric sensing device 212. The processing device 200 can be implemented as any electronic device capable of processing, receiving, or transmitting data or instructions. For example, the processing device 200 can be a microprocessor, a central processing unit (CPU), an application-specific integrated circuit (ASIC), a digital signal processor (DSP), or combinations of such devices. As described herein, the term "processing device" is meant to encompass a single processor or processing unit, multiple processors, multiple processing units, or other suitably configured computing element or elements.

[0030] The memory 202 can store electronic data that can be used by the electronic device 100. For example, a memory can store electrical data or content such as, for example, audio and video files, documents and applications, device settings and user preferences, timing signals, biometric images, data structures or databases, and so on. The memory 202 can be configured as any type of memory. By way of example only, the memory can be implemented as random access memory, read-only memory, Flash memory, removable memory, or other types of storage elements, or combinations of such devices.

[0031] The I/O device 204 can transmit and/or receive data to and from a user or another electronic device. One example of an I/O device is button 106 in FIG. 1. The I/O device(s) 204 can include a display, a touch sensing input surface such as a trackpad, one or more buttons, one or more microphones or speakers, one or more ports such as a microphone port, and/or a keyboard.

[0032] The electronic device 100 may also include one or more sensors 206 positioned substantially anywhere on the electronic device 100. The sensor or sensors 206 may be configured to sense substantially any type of characteristic, such as but not limited to, images, pressure, light, touch, heat, movement, relative motion, biometric data, and so on. For example, the sensor(s) 208 may be an image sensor, a heat sensor, a light or optical sensor, an accelerometer, a pressure transducer, a gyroscope, a magnet, a health monitoring sensor, and so on.

[0033] The power source 208 can be implemented with any device capable of providing energy to the electronic device 100. For example, the power source 208 can be one or more batteries or rechargeable batteries, or a connection cable that connects the remote control device to another power source such as a wall outlet.
[0034] The network communication interface 210 can facilitate transmission of data to or from other electronic devices. For example, a network communication interface can transmit electronic signals via a wireless and/or wired network connection. Examples of wireless and wired network connections include, but are not limited to, cellular, Wi-Fi, Bluetooth, IR, and Ethernet.

[0035] The biometric sensing device 212 can be implemented as any suitable biometric sensor, scanner, and/or system. For example, the biometric sensing device can be a facial recognition device, an iris or retina scanner, a vein recognition device that can image the veins in a finger or palm, a facial biometrics scanner, and/or a thermal imaging scanner. In embodiments described herein, the biometric sensing device can be one or more fingerprint sensors. The fingerprint sensor can capture images one or more fingers, a portion of one or more fingers, and/or some or all of a palm or of a hand. In some embodiments, the fingerprint sensor is positioned at a location that a user's finger, fingers and/or hands are naturally in contact with as the user interacts with the electronic device. For example, an electronic device can include a fingerprint sensor in the display 104, the button 106, the enclosure 102, and/or as a separate electronic device that is connected to the electronic device 100. Additionally, the fingerprint sensor can be implemented with any suitable sensing technology, including, but not limited to, capacitive, resistive, ultrasound, piezoelectric, and thermal sensing technology.

[0036] It should be noted that FIGS. 1 and 2 are illustrative only. In other examples, an electronic device may include fewer or more components than those shown in FIGS. 1 and 2.

[0037] A fingerprint sensor will be used to describe various embodiments, with the fingerprint sensor including a capacitive fingerprint sensor. One example construction of a capacitive fingerprint sensor and how the capacitive fingerprint sensor captures a fingerprint is now briefly described. FIG. 3 illustrates an enlarged and simplified cross-section view of a portion of a fingerprint sensor taken along line 3-3 in FIG. 1. A first layer 310 can be disposed over a dielectric layer 320. By way of example only, the first layer 310 can be a dielectric layer such as an exterior surface of a button or other input device (e.g., button 106 in FIG. 1), an exterior surface of an input device such as a trackpad or mouse, and/or a cover glass of a display (e.g., display 104 in FIG 1). In some embodiments, the dielectric layer 320 can be a color layer that can be used to reduce the visibility of the electrodes and other circuitry of the fingerprint sensor.
[0038] The capacitive fingerprint sensor 300 can capture a fingerprint image of at least a portion of the finger 302 by measuring capacitance differences between the finger 302 and the electrodes 314. A fingerprint is generally formed from ridges 304 and valleys 306 arranged in a unique pattern. Typically, the capacitance measured between a ridge 304 and one or more electrodes 314 varies from the capacitance measured between a valley 306 and one or more electrodes 314. The measured capacitance between a ridge and an electrode can be greater than the measured capacitance between a valley and an electrode because the ridge is closer to the electrode. The differences in the measured capacitances can be used to distinguish between ridges and valleys and produce a fingerprint image.

[0039] The skin on the finger 302 includes a dead skin layer 316 disposed over a live skin layer 318. The capacitive fingerprint sensor 300 typically images the dead skin layer 316 to obtain an image of the fingerprint. However, if a portion of the dead skin layer 316 is damaged or missing, the capacitive fingerprint sensor can obtain an image of the fingerprint by imaging the live skin layer 318 by itself, or by imaging both the remaining dead skin layer 316 and the exposed live skin layer 318.

[0040] Referring now to FIG. 4, there is shown a flowchart of a method capturing fingerprint images. The fingerprint images can be captured in the background while a user interacts naturally with an electronic device, thereby reducing or eliminating the need to perform an explicit fingerprint enrollment process. Initially, a determination is made at block 400 as to whether or not a user has given their permission for the fingerprint sensor to capture fingerprint images in the background. By way of example only, a user can grant permission through a setting associated with the fingerprint sensor, and/or the user can be asked if he or she wants the fingerprint sensor to capture images in the background during a setup process that can occur when the user first uses the electronic device. The method ends if the user does not give permission.

[0041] When a user has granted permission to capture his or her fingerprint images in the background, the process passes to block 402 where a determination is made as to whether the user, or a finger of the user, has contacted an input region of the fingerprint sensor. As one example, an input region of a fingerprint sensor can be the exterior surface of button 106 in FIG. 1. Additionally or alternatively, an input region can be a predetermined location on the display 104, or the input region can be any location on the entire display 104. In some embodiments, a fingerprint sensor can capture a fingerprint image when a finger is in contact
with, or in close proximity to, the input region of the fingerprint sensor. If the user has not contacted the input region, the method waits at block 402 until the user contacts the input region of the fingerprint sensor.

[0042] When the user contacts the input region of the fingerprint sensor, the process continues at block 404 where a fingerprint image is captured. A determination is then made at block 406 as to whether the user has withdrawn his or her permission to acquire fingerprint images in the background. If not, the method returns to block 402. When the user withdraws his or her permission, the fingerprint sensor ceases to capture fingerprint images in the background and the method ends.

[0043] FIG. 5 is a flowchart of a method for associating a fingerprint image captured in the background with a user. The illustrated method can be performed after a user has given permission for the fingerprint sensor to capture fingerprint images in the background. Initially, at block 500, a fingerprint image can be captured when the user contacts (or is in close proximity to) the input region of the fingerprint sensor. A determination is then made at block 502 as to whether the user has entered user identification data (UID) within a given period of time around the time the fingerprint image is captured. The given time period can be a predetermined time period or a user can select the time period. The UID can be a pin or password in some embodiments. For example, a pin or password can be used to unlock the electronic device or to access to an application or a website using the electronic device.

[0044] If the UID is entered within the given time period, the process continues at block 504 where the fingerprint image is tagged with the UID and the tagged fingerprint image is assigned to a cluster. When the user does not enter a UID within the given time period, the method passes to block 506 where the untagged fingerprint image is assigned to a cluster. In one embodiment, multiple clusters can be created, with each cluster containing one or more fingerprint images for a respective finger. Thus, one cluster can contain fingerprint images of one finger (e.g., the left index finger) while another cluster can include fingerprint images of another finger (e.g., the right index finger).

[0045] In other embodiments, a cluster can include fingerprint images based on different criterion. As one example, clusters can correspond to different parts of the same finger. One cluster can include images associated with the tip of a finger while another cluster includes images that correspond to a core area of the same finger.
In some embodiments, a new fingerprint image can be assigned to a cluster when the newly captured fingerprint image matches a previously captured fingerprint image. The previously captured fingerprint image may or may not be tagged with the UID. FIG. 6 illustrates one method for assigning fingerprint images to a cluster. As described earlier, a number of fingerprint images 600, 602, 604, 606, and 608 can be assigned to a cluster when the fingerprint images correspond to the same finger. A newly captured fingerprint image can be compared and cross-matched to all of the previously captured fingerprint images. When the new fingerprint image is matched to at least a portion of an existing fingerprint image in a cluster, then the new fingerprint image is included in that cluster.

Those skilled in the art will recognize that the other embodiments can perform the method shown in FIG. 5 differently. As one example, fingerprint images that are not tagged with a UID can be deleted and not assigned to a cluster. In this embodiment, the clusters are limited to tagged fingerprint images. In another embodiment, untagged fingerprint images can be assigned to different clusters than tagged fingerprint images. Thus, the fingerprint images in each cluster will include only tagged fingerprint images or only untagged fingerprint images.

The method of FIG. 5 will now be described with reference to an example application. When a user enables a passcode locking feature in an electronic device, such as in a smart telephone, the user must enter a pin or some other UID to unlock the electronic device. The unlock procedure can include the user first pressing a button (e.g., button 106 in FIG. 1) and then entering a pin. When a fingerprint sensor is included in the button, a fingerprint image can be acquired when the user presses the button. If the user enters the pin within a given time period after pressing the button, the fingerprint image that was captured when the user pressed the button is tagged with the pin and assigned to a cluster (e.g., the cluster for the finger used to press the button). Subsequently, the next time the user wants to unlock the electronic device, the user presses the button and another fingerprint image is captured. If the newly captured fingerprint image matches the fingerprint image tagged with the pin, the electronic device is unlocked immediately. The user does not have to enter the pin to unlock the electronic device.

Referring now to FIG. 7, there is shown a method for authenticating a user using a previously captured and tagged fingerprint image. Initially, a fingerprint image is captured at block 700 when a finger of a user is in contact with, or is in close proximity to, an input region of the fingerprint sensor. As one example, a user can press a button or a key on a keyboard, an exterior surface of a button, a trackpad, or a mouse. The user can be unlocking the electronic
device, opening an application, entering a website address, or switching from one application to another application.

[0050] A determination is then made at block 702 as to whether the newly captured fingerprint image matches a tagged cluster. In one embodiment, the newly captured fingerprint image may match a tagged fingerprint image in a cluster. In another embodiment, the newly captured fingerprint image can match an untagged fingerprint image in a cluster that includes at least one tagged fingerprint image.

[0051] Additionally, in some embodiments, multiple users can interact with the same electronic device. When more than one user has given his or her permission to capture fingerprint images in the background, one or more clusters can be associated with each user. Thus, in block 702, the determination as to whether the newly captured fingerprint image matches a tagged cluster can be limited to those clusters that are associated with the current user of the electronic device. Other embodiments can compare and cross-match the newly captured fingerprint image with fingerprint images in all of the tagged clusters.

[0052] If the newly captured fingerprint image matches a tagged cluster, the process passes to block 704 where the newly captured fingerprint image can be assigned to a cluster. At block 706, the identity of the user is authenticated and the user is given access to the electronic device, or to the application being accessed on the electronic device. Thus, the step of entering a UID can be eliminated. The user does not have to enter a UID to have access to the device, application, or website when the newly captured fingerprint image matches a tagged cluster.

[0053] Next, as shown in block 708, the electronic device, application, and/or website can be configured for the current user based on his or her preferences. For example, when a user unlocks an electronic device, the home screen, icons, wallpaper, and other features can be presented to the user based on his or her preferences. Thus, multiple users of a single electronic device, such as a family tablet computer, can each view the home screen, applications, and other functions as specified by that user. As one example, the bookmarks in a web browsing application can be provided to each user based on their individually selected bookmarks. Additionally, the icons, as well as the layout of the icons, can be displayed to each user based on their preferences.
Returning again to block 702, if the newly captured image does not match a tagged cluster, the method continues at block 502. Blocks 502, 504, and 506 can be performed as described earlier in conjunction with FIG. 5. The method of FIG. 7 ends after the newly captured fingerprint image is assigned to a cluster.

Other embodiments can perform the method shown in FIG. 7 differently. Blocks can be added, performed in a different order, and/or some blocks can be omitted. For example, in some embodiments, block 704 and/or block 708 can be omitted.

One example of a multi-user environment will now be described. Several family members can share a tablet computing device and each family member can have his or her own account on a social networking website. Over time, as the family members interact naturally with the tablet, fingerprint images of each family member can be acquired automatically and in the background, and the fingerprint images of the family members tagged with their respective UID's for their social networking accounts. The tagged fingerprint images can be assigned to clusters associated with each family member. User authentication can then be done in the background, with the user given access to his or her social networking account without having to enter a password. A new fingerprint image of a family member currently using the electronic device can be captured when the user opens the social networking website and/or when the user switches to the social networking website. If the new fingerprint image matches a tagged cluster for the social networking account, and optionally that tagged fingerprint image is assigned to a cluster associated with that family member, the social networking account can be opened and made accessible to the user immediately. Thus, the social networking account may be opened using a tagged cluster and not by the user entering his or her UID (e.g., password).

Additionally, in some embodiments, a second family member who is trying to log into his or her social network account when another family member unlocked the device may not be able to do so because his or her fingerprint images will not match any of the fingerprint images in the cluster(s) associated with the family member that unlocked the device. In other embodiments, when the review is not limited to the clusters associated with the family member that unlocked the electronic device and all of the tagged clusters are reviewed, the second family member may be given access to his or her social network account immediately if their fingerprint image matches a tagged cluster.
[0058] A cluster can be a connected component of a set of images. For example, a cluster can correspond to data from a single finger only, or a cluster can correspond to a single user.

FIGS. 8-9 depict methods for combining fingerprint images or tags in different clusters. FIG. 8 depicts two clusters, cluster 1 and cluster 2. Cluster 1 includes two tagged fingerprint images; one image is tagged with a first UID and the other fingerprint image with a second UID. As one example, the first UID can be associated with a passcode used to unlock the device while the second UID with a website, such as an online banking website.

[0059] Cluster 2 also includes two tagged fingerprint images; one image is tagged with the first UID and the other fingerprint image with a third UID. As another example, the third UID can be associated with another website, such as a social networking website.

[0060] Because one fingerprint image in both clusters is tagged with the first UID tag, the UID2 and UID3 tags can migrate to the other respective cluster. The third UID tag can migrate to cluster 1 while the second UID tag can migrate to cluster 2. Both cluster 1 and cluster 2 have three UID tags instead of the initial two UID tags.

[0061] In some embodiments, two clusters that are associated with the same user can be assigned to a user cluster. For example, Cluster 1 can include multiple fingerprint images F1 and F2 associated with the same finger with the same part of the same finger. Cluster 2 can include multiple fingerprint images F3 and F4 that are associated with a different or with a different part of a different finger. Cluster 1 and cluster 2 can be assigned to the same user cluster when the two clusters are associated with the same user. Thus, a user cluster can include several finger clusters of the same user.

[0062] And in yet another embodiment, two or more clusters can be merged into one cluster when a new fingerprint image matches at least one image in each cluster. As one example, two clusters can be merged into a single cluster when the two clusters correspond to different parts of the same finger.

[0063] Referring now to FIG. 10, there is shown a flowchart of a method for deleting fingerprint images. In some embodiments, only a predetermined number of fingerprint images can be saved and assigned to one or more clusters. The method shown in FIG. 10 can be performed when a new fingerprint image is acquired and the maximum number of fingerprint images has been captured and stored. This embodiment considers only untagged fingerprint images, the size of a cluster, and the extent of overlap in overlapping fingerprint images when deleting
fingerprint images. Other embodiments can consider additional or different factors, such as the quality of a fingerprint image and/or the fingerprint images associated with the least used UID tags. As another example, tagged fingerprint images can be deleted in embodiments that associated tags to the cluster or clusters that include the tagged fingerprint images.

[0064] Initially, a determination is made as to whether the maximum number of fingerprint images has been captured. If not, the method waits until the maximum number of fingerprint images is captured and stored. When the maximum number of fingerprint images is saved, the process passes to block 1002 where a determination is made as to whether a new fingerprint image has been captured. If not, the method returns to block 1000.

[0065] When a new fingerprint image is captured, the process continues at block 1004 where a determination can be made as to whether any untagged fingerprint images are stored in one or more clusters. If so, at least one untagged fingerprint image can be deleted at block 1006 and the method passes to block 1008 where the newly captured fingerprint image can be assigned to a cluster. The method can end after the newly captured fingerprint image is assigned to a cluster.

[0066] If there are no untagged fingerprint images stored in one or more clusters, the method continues at block 1010 where a determination is made as to whether fingerprint images are to be deleted from a cluster having the fewest number of fingerprint images. If so, at least one fingerprint image in the cluster with the fewest number of fingerprint images can be deleted and the newly captured fingerprint image assigned to a respective cluster (blocks 1006 and 1008).

[0067] When fingerprint images are not to be deleted from a cluster having the fewest number of fingerprint images, the process passes to block 1012 where one or more least valuable images are deleted. In some embodiments, a fingerprint image can be considered less valuable when the fingerprint image does not contribute additional information to the cluster. The newly captured image can then be saved and assigned to the same cluster or to a different cluster at block 1008.

[0068] As described previously, biometric sensing devices other than fingerprint sensors can be included or connected to an electronic device. Thus, images or data relating to other types of biometric attributes can be used in other embodiments. For example, a user's face, veins, retina, iris, and thermal images can be captured in the background as the user interacts with the
electronic device. Additionally, images or data of the biometric attributes can be used to authenticate a user in the background.

[0069] Various embodiments have been described in detail with particular reference to certain features thereof, but it will be understood that variations and modifications can be effected within the spirit and scope of the disclosure. And even though specific embodiments have been described herein, it should be noted that the application is not limited to these embodiments. In particular, any features described with respect to one embodiment may also be used in other embodiments, where compatible. Likewise, the features of the different embodiments may be exchanged, where compatible.
What is claimed is:

1. A method for authenticating a user of an electronic device that includes a biometric sensing device, the method comprising:
   - capturing at a first time a first biometric image when the user interacts with the electronic device;
   - tagging the first biometric image with a first user identification data (UID) that is associated with the user;
   - capturing at a second time a second biometric image when the user interacts with the electronic device;
   - determining if the second biometric image matches the first biometric image tagged with the first UID; and
   - allowing the user to access the electronic device or an application on the electronic device when the second biometric image matches the tagged first biometric image.

2. The method as in claim 1, further comprising:
   - capturing at a third time a third biometric image when the user interacts with the electronic device;
   - determining if the third biometric image matches either the first biometric image or the second biometric image; and
   - allowing the user to access the electronic device or an application on the electronic device when the third biometric image matches either the first biometric image or the second biometric image.

3. The method as in claim 1, wherein tagging the first biometric image with a first user identification data (UID) comprises tagging the first biometric image with a first user identification data (UID) when the user enters the first UID within a given time period of the first biometric image being captured.

4. The method as in claim 1, wherein the first and second biometric images each comprise a fingerprint image.

5. The method as in claim 1, further comprising assigning the first biometric image tagged with the first UID to a cluster, wherein each cluster is associated with a respective biometric attribute of the user.
6. The method as in claim 1, further comprising tagging the second biometric image with a second UID when the user enters a second UID within a given time period of the second biometric image being captured.

7. The method as in claim 6 further comprising assigning the second biometric image tagged with the second UID to a cluster.

8. The method as in claim 1, further comprising assigning the second biometric image to a cluster when the user does not enter the second UID within the given time period.

9. The method as in claim 6, wherein the second UID and the first UID comprise the same UID.

10. The method as in claim 5, further comprising:
    prior to assigning the first biometric image tagged with the first UID to the cluster,
    determining if a maximum number of biometric images have been assigned to one or more clusters;
    selecting one or more biometric images to be deleted when the maximum number of biometric images have been assigned to one or more clusters; and
    deleting at least one biometric image.

11. The method as in claim 10, wherein at least one biometric image is selected to be deleted based on an amount of contribution the at least one biometric image contributes to the assigned cluster.

12. The method as in claim 1, further comprising:
    repeatedly capturing biometric images when the user interacts with the electronic device;
    and
    repeatedly tagging each biometric image with a respective UID when the UID is entered within the given time period of the capture of the biometric image.

13. The method as in claim 12, further comprising:
    determining whether two clusters each include a biometric image tagged with the same UID;
    if so, determining whether one of the two clusters includes a biometric image tagged with a different UID; and
    migrating the different UID into the cluster that does not include the different UID.
14. An electronic device, comprising:
a processing device; and
a biometric sensing device operatively connected to the processing device, wherein the biometric sensing device is configured to capture biometric images when a user interacts with the electronic device and the processing device is configured to receive at least one biometric image and tag the at least one biometric image with a user identification data (UID) entered by the user within a given time period around the capture of the at least one biometric image.

15. The electronic device as in claim 14, wherein the biometric sensing device comprises a fingerprint sensor.

16. The electronic device as in claim 15, wherein the fingerprint sensor is included in a button on the electronic device.

17. The electronic device as in claim 15, further comprising a display operatively connected to the processing device, wherein the fingerprint sensor is included in at least a portion of the display.

18. A method for authenticating multiple users of an electronic device that includes a biometric sensing device, the method comprising:
capturing a first biometric image when a first user interacts with the electronic device;
tagging the first biometric image with a first user identification data (UID) associated with the first user;
assigning the first biometric image tagged with the first UID to a cluster associated with the first user, wherein each cluster associated with the first user corresponds to a respective biometric attribute of the first user;
capturing a second biometric image when the first user interacts with the electronic device;
and
allowing the first user access to the electronic device or to an application on the electronic device when the second biometric image matches the first biometric image tagged with the first UID.

19. The method as in claim 18, further comprising:
if the second biometric image does not match the first biometric image tagged with the first UID, tagging the second biometric image with a second UID associated with the first user;
capturing a third biometric image when the first user interacts with the electronic device;

and

allowing the first user access to the electronic device or to an application on the electronic device when the third biometric image matches the first biometric image tagged with the first UID or the second biometric image tagged with the second UID.

20. The method as in claim 19, further comprising:
capturing a fourth biometric image when a second user interacts with the electronic device;
tagging the fourth biometric image with a third UID associated with the second user;
assigning the fourth biometric image tagged with the third UID to a cluster associated with the second user, wherein each cluster associated with the second user corresponds to a respective biometric attribute of the second user;
capturing a fifth biometric image when the second user interacts with the electronic device; and
allowing the second user access to the electronic device or to an application on the electronic device when the fifth biometric image matches the fourth biometric image tagged with the third UID.

21. The method as in claim 20, further comprising:
capturing a sixth biometric image when the second user interacts with the electronic device;
determining if the fifth biometric image matches either the fifth biometric image or the fourth biometric image; and
allowing the second user to access the electronic device or an application on the electronic device when the sixth biometric image matches either the fifth biometric image or the fourth biometric image.

22. The method as in claim 18, further comprising:
capturing a fifth biometric image when the first user interacts with the electronic device;
determining if the fifth biometric image matches either the first biometric image or the second biometric image; and
allowing the first user to access the electronic device or an application on the electronic device when the fifth biometric image matches either the first biometric image or the second biometric image.
Start

User Permission? 400

No

Contact Sensor? 402

Yes

Capture Fingerprint Image 404

No

Permission Withdrawn? 406

Yes

Stop Capturing Fingerprint Images 408

Stop

FIG. 4
Start

Capture Fingerprint Image When User Contacts Input Region Of Fingerprint Sensor 500

Enter UID In Time? 502

No → Assign Untagged Fingerprint Image To A Cluster 506

Yes → Tag Fingerprint Image With UID And Assign Tagged Fingerprint Image To A Cluster 504

Stop

FIG. 5

FIG. 6
Start

No

Maximum Images? 1000

Yes

No

Capture New Image? 1002

Yes

No

Untagged Images? 1004

Yes

No

Cluster Size? 1010

Yes

Delete Fingerprint Image 1006

No

Delete Least Valuable Image 1012

Assign Newly Captured Fingerprint Image To A Cluster 1008

Stop

FIG. 10
### A. CLASSIFICATION OF SUBJECT MATTER

**INV. G06F 21/32**

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

### C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>paragraphs [0017], [0067], [0080]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[0081]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraphs [0021], [0059]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0060]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraphs [0070], [0075]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>figures 1-7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the whole document</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the whole document</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-/-</td>
<td></td>
</tr>
</tbody>
</table>

[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) one of 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 considered in conjunction with one or more other such documents, such combination being obvious to a person skilled in the art
  
* "Z" document member of the same patent family

### Date of the actual completion of the international search

14 October 2014

### Date of mailing of the international search report

22/10/2014

### Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040,  
Fax: (+31-70) 340-3016

Authorized officer

Frank, Mari o

Form PCT/ISA/210 (second sheet) (April 2005)
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>US 2012331566 AI</td>
<td>27-12-2012</td>
<td>DE 112012002579 T5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GB 2505801 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2012331566 AI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2012174664 AI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2007229385 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 20070090703 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2008113685 AI</td>
</tr>
<tr>
<td>US 2005169503 AI</td>
<td>04-08-2005</td>
<td>US 2005169503 AI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2005072372 A2</td>
</tr>
<tr>
<td>EP 1521161 A2</td>
<td>06-04-2005</td>
<td>CN 1612081 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1521161 A2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2005071635 AI</td>
</tr>
</tbody>
</table>