Claims

1. A two stage method for logging a first user in to a mobile computing device being in a locked mode, said method comprising:

(a) storing data associated with the first user and storing information that relates to a facial image of that first user, at a memory of the mobile computing device;

(b) when the mobile computing device is in a locked mode:

(b.1) receiving data inserted by a user who wishes to unlock the mobile computing device;

(b.2) comparing the received data with the stored data associated with the first user and determining whether the received data matches the stored data associated with the first user;

(b.3) if it has been determined that the received data matches the stored data associated with the first user, prompting an image capturing device associated with the mobile computing device to capture a facial image of the user who inserted the data received;

(b.4) retrieving information that relates to a facial image of the user who inserted the received data and comparing that information with information that had been stored at the memory of the mobile computing device, wherein the latter information relates to the facial image of that first user;

(c) if the retrieved information relating to a facial image of the user who inserted the received data matches the information relating to the facial image of the first user which has been stored at the memory of the mobile computing device, unlocking the mobile computing device.

2. The method of claim 1, wherein in case the image captured in step b.3 cannot be used for extracting enough information in order to carry out a matching process with the information relating to the facial image of the first user which has been stored at the memory of the mobile computing device, the method further comprises the steps of:

(d.1) enabling limited access to resources of the mobile computing device;

(d.2) triggering the image capturing device to capture another image and processing the newly captured image; and

(d.3) if the newly captured image cannot be used for extracting enough information in order to carry out a matching process with the information relating to the facial image of the first user which had been stored at the memory of the mobile computing device, repeating steps d.2 and d.3 for up to a pre-defined number of times; and

(d.4) if following that pre-defined number of times, no match has been found between the extracted information and the information relating to the facial image of the first user which had been stored at the memory of the mobile computing device, logging off the user who was granted with a limited access to the mobile computing device.

3. The method according to claim 2, wherein step d.2 is repeated for up to a pre-defined number as long as not enough information can be extracted from the newly captured image in order to carry out a matching process with the information relating to the facial image of the first user which has been stored at the memory of the mobile computing device, and wherein hitting of a key at the mobile computing device keyboard or making a gesture

at a touch sensitive area of the mobile computing device, triggers capturing of a new image.

4. The method according to claim 1, wherein if the retrieved information relating to a facial image of the user who inserted the received data has been successfully processed but does not match the information relating to the facial image of the first user which had been stored at the memory of the mobile computing device, denying access to the mobile computing device resources from the user whose facial image has been captured and processed.

5. The method according to claim 1, wherein the retrieval of information that relates to a facial image of the user comprises processing the facial image to identify therefrom at least one characteristic of the user.

6. The method according to claim 1, wherein the processing of the facial image comprises extracting at least one unique facial signature from the user facial image and matching each of the at least one extracted unique signatures with facial signatures related data comprised in the memory of the mobile computing device.

7. The method according to claim 1, wherein the processing of the facial image is carried out by using an image capturing device which is different from the image capturing device operatively coupled with the mobile computing device, for generating the information that relates to a facial image of the first user that has been stored at a memory of the mobile computing device.

8. A two stage method for logging a first user in to a mobile computing device, comprising:

(a) storing at the memory of the mobile computing device user identification data of two types, wherein the first type of identification data is characterized in that it consumes a small amount of resources of the mobile computing device for comparing the stored identification data of the first type with data of the first type that would be introduced to the mobile computing device, and wherein the second type of identification data is characterized in that it consumes a substantially larger amount of the mobile computing device resources than the identification data of the first type, for comparing the stored identification data of the second type with data of the second type that would be introduced to the mobile computing device;

(b) when the mobile computing device is in a locked mode:

(b.1) receiving data of the first type, inserted by a user who wishes to unlock the mobile computing device;

(b.2) comparing the received data of the first type with the stored identification data of the first type associated with said first user, and determining whether the received data of the first type matches the stored identification data of the first type;

(b.3) if it has been determined that the received data of the first type matches the stored identification data of the first type associated with the first user, enabling capturing of data of the second type associated with the user who wishes to unlock the mobile computing device;

(b.4) using the captured data of the second type for matching same with identification data of the second type associated with the first user, that had

been stored at the memory of the mobile computing device;

(c) if it has been determined that the received data of the second type matches the stored identification data of the second type associated with the first user, unlocking the mobile computing device.

9. The method of claim 8, wherein the identification data of the second type stored in the mobile computing device comprises data that belongs to at least two different classes of data.

10. The method of claim 9, further comprising a step wherein if the captured data of the second type does not contain enough information for matching same with identification data of the second type associated with the first user that had been stored at the memory of the mobile computing device, step b.3 comprises enabling capturing of data with the user who wishes to unlock the mobile computing device, wherein said data belongs to a different class of the second type which is different from the captured data of the second type that did not contain enough information for carrying out the matching process.

11. A mobile computing device comprising:
a power source;
an image capturing device;
a user interface configured to enable a user to insert a password;
a memory or storage device storing: a) a password associated with the first user; b) information that relates to a facial image of the first user; c) a program;
one or more processing units operable to execute the program, wherein the execution of the program causes the

one or more processing units to carry out the following operations when the mobile computing device is in a locked mode:

to process data inserted via the user interface by a user who wishes to unlock the mobile computing device;

to compare the inserted data with the password associated with the first user that has been stored at the memory or storage device and to determine whether the inserted data matches the password associated with the first user;

if the inserted data matches the password associated with the first user, prompting the image capturing device to capture a facial image of the user who inserted the data;

to retrieve information that relates to a facial image of the user who inserted the data and to compare that information with information that has been stored at the memory or storage device, wherein the latter information relates to the facial image of the first user;

if the retrieved information which relates to a facial image of the user who inserted the data matches the information which has been stored at the memory or storage device and relates to the facial image of the first user, prompting the unlock of the mobile computing device.

12. The mobile computing device according to claim 11, wherein in case the facial image of the user who inserted the data that was captured by the image capturing device, cannot be used for extracting enough information in order to carry out a matching process with the information relating to the facial image of the first user which had

been stored at the memory of the mobile computing device, the one or more processing units are further configured to carry out the following operations:

to enable limited access to resources of the of the mobile computing device;

to prompt the image capturing device to capture another image and to process the newly captured image; and

if the newly captured image cannot be used for extracting enough information in order to carry out a matching process with the information relating to the facial image of the first user which had been stored at the memory of the mobile computing device, repeating the steps of capturing the image and processing it for up to a pre-defined number of times; and

if after that pre-defined number of times, no match has been found between the extracted information and the information relating to the facial image of the first user which has been stored at the memory of the mobile computing device, to automatically log off the user to a limited access to the mobile computing device was granted.

13. The mobile computing device according to claim 12, wherein the one or more processing unit are configured to repeat prompting the image capturing device to capture an image and to process it for up to a pre-defined number of times, as long as the newly captured image cannot be applied for extracting enough information in order to carry out a matching process with the information relating to the facial image of the first user which has been stored at the memory of the mobile computing device, and wherein hitting a key at the mobile computing device keyboard or making a gesture at a touch sensitive area of the mobile computing device, triggers the prompting of capturing a new image.

14. The mobile computing device according to claim 11, wherein if the retrieved information relating to a facial image of the user who inserted the received data has been successfully processed but does not match the information relating to the facial image of the first user which had been stored at the memory of the mobile computing device, the one or more processing units are configured to deny access to the mobile computing device resources from the user whose facial image has been captured and processed.

15. A computer program product stored on a non-transitory tangible computer readable medium and comprising instructions that, when executed, cause a mobile computing device comprising one or more computer processors to perform a method according to claim 1.

16. The computer program product according to claim 15, wherein in case the captured facial image captured cannot be used for extracting enough information in order to carry out a matching process with the information relating to the facial image of the first user which has been stored at the memory of the mobile computing device, the method further comprises the steps of:

(i) enabling limited access to resources of the of the mobile computing device;

(ii) triggering the image capturing device to capture another image and processing the newly captured image; and

(iii) if the newly captured image cannot be used for extracting enough information in order to carry out a matching process with the information relating to the facial image of the first user which had been stored at the memory of the mobile computing device, repeating steps d.2 and d.3 for up to a pre-defined number of times; and

(iv) if after that pre-defined number of times, no match has been found between the extracted information the information relating to the facial image of the first user which has been stored at the memory of the mobile computing device, logging off the user who was granted with a limited access to the mobile computing device.

Claims

1. A two stage method for logging a first user in to a mobile computing device being in a locked mode, said method comprising:

(a) storing data associated with the first user and storing information that relates to a facial image of that first user, at a memory of the mobile computing device;

(b) when the mobile computing device is in a locked mode:

(b.1) receiving data inserted by a user who wishes to unlock the mobile computing device;

(b.2) comparing the received data with the stored data associated with the first user and determining whether the received data matches the stored data associated with the first user;

(b.3) if it has been determined that the received data matches the stored data associated with the first user, prompting an image capturing device associated with the mobile computing device to capture a facial image of the user who inserted the data received;

(b.4) retrieving information that relates to a facial image of the user who inserted the received data and comparing that information with information that had been stored at the memory of the mobile computing device, wherein the latter information relates to the facial image of that first user;

(c) if the retrieved information relating to a facial image of the user who inserted the received data matches the information relating to the facial image of the first user which has been stored at the memory of the mobile computing device, unlocking the mobile computing device,

and wherein in case the image captured in step b.3 cannot be used for extracting enough information in order to carry out a matching process with the information relating to the facial image of the first user which has been stored at the memory of the mobile computing device, the method further comprises the steps of:

(d.1) enabling limited access to resources of the mobile computing device;

(d.2) triggering the image capturing device to capture another image and processing the newly captured image; and

(d.3) if the newly captured image cannot be used for extracting enough information in order to carry out a matching process with the information relating to the facial image of the first user which had been stored at the memory of the mobile computing device, repeating steps d.2 and d.3 for up to a pre-defined number of times; and

(d.4) if following that pre-defined number of times, no match has been found between the extracted information and the information relating to the facial image of the first user which had been stored at the memory of the mobile computing device, logging off the user who was granted with a limited access to the mobile computing device.

2. The method according to claim 1, wherein step d.2 is repeated for up to a pre-defined number as long as not enough information can be extracted from the newly captured image in order to carry out a matching process with the information relating to the facial image of the first user which has been stored at the memory of the mobile computing device, and wherein hitting of a key at the mobile computing device keyboard or making a gesture at a touch sensitive area of the mobile computing device, triggers capturing of a new image.

3. The method according to claim 1, wherein if the retrieved information relating to a facial image of the user who inserted the received data has been successfully processed but does not match the information relating to the facial image of the first user which had been stored at the memory of the mobile computing device, denying access to the mobile computing device resources from the user whose facial image has been captured and processed.

4. The method according to claim 1, wherein the retrieval of information that relates to a facial image of the user comprises processing the facial image to

identify therefrom at least one characteristic of the user.

5. The method according to claim 1, wherein the processing of the facial image comprises extracting at least one unique facial signature from the user facial image and matching each of the at least one extracted unique signatures with facial signatures related data comprised in the memory of the mobile computing device.

6. The method according to claim 1, wherein the processing of the facial image is carried out by using an image capturing device which is different from the image capturing device operatively coupled with the mobile computing device, for generating the information that relates to a facial image of the first user that has been stored at a memory of the mobile computing device.

7. A mobile computing device comprising:
a power source;
an image capturing device;
a user interface configured to enable a user to insert a password;
a memory or storage device storing: a) a password associated with the first user; b) information that relates to a facial image of the first user; c) a program;
one or more processing units operable to execute the program, wherein the execution of the program causes the one or more processing units to carry out the following operations when the mobile computing device is in a locked mode:

to process data inserted via the user interface by a user who wishes to unlock the mobile computing device;

to compare the inserted data with the password associated with the first user that has been stored at the memory or storage device and to determine whether the inserted data matches the password associated with the first user;

if the inserted data matches the password associated with the first user, prompting the image capturing device to capture a facial image of

the user who inserted the data;

to retrieve information that relates to a facial image of the user who inserted the data and to compare that information with information that has been stored at the memory or storage device, wherein the latter information relates to the facial image of the first user;

if the retrieved information which relates to a facial image of the user who inserted the data matches the information which has been stored at the memory or storage device and relates to the facial image of the first user, prompting the unlock of the mobile computing device,

and wherein in case the facial image of the user who inserted the data that was captured by the image capturing device, cannot be used for extracting enough information in order to carry out a matching process with the information relating to the facial image of the first user which had been stored at the memory of the mobile computing device, the one or more processing units are further configured to carry out the following operations:

to enable limited access to resources of the of the mobile computing device;

to prompt the image capturing device to capture another image and to process the newly captured image; and

if the newly captured image cannot be used for extracting enough information in order to carry out a matching process with the information relating to the facial image of the first user which had been stored at the memory of the mobile computing device, repeating the steps of capturing the image and processing it for up to a pre-defined number of times; and

if after that pre-defined number of times, no match has been found between the extracted information and the information relating to the facial image of the first user which has been stored at the memory of the mobile computing device, to automatically log off the user to a limited access to the mobile computing device was granted.

8. The mobile computing device according to claim 7, wherein the one or

more processing unit are configured to repeat prompting the image capturing device to capture an image and to process it for up to a pre-defined number of times, as long as the newly captured image cannot be applied for extracting enough information in order to carry out a matching process with the information relating to the facial image of the first user which has been stored at the memory of the mobile computing device, and wherein hitting a key at the mobile computing device keyboard or making a gesture at a touch sensitive area of the mobile computing device, triggers the prompting of capturing a new image.

9. The mobile computing device according to claim 7, wherein if the retrieved information relating to a facial image of the user who inserted the received data has been successfully processed but does not match the information relating to the facial image of the first user which had been stored at the memory of the mobile computing device, the one or more processing units are configured to deny access to the mobile computing device resources from the user whose facial image has been captured and processed.