(12) **PATENT**

(11) **347923** (13) **B1**

NORWAY

(19) NO

(51) Int Cl.

G06F 21/32 (2013.01)
G06F 21/44 (2013.01)
G06F 21/57 (2013.01)
G06V 10/143 (2022.01)
G06V 20/00 (2022.01)
G06V 40/16 (2022.01)
G06V 40/40 (2022.01)
H04W 12/02 (2009.01)
H04W 12/065 (2021.01)

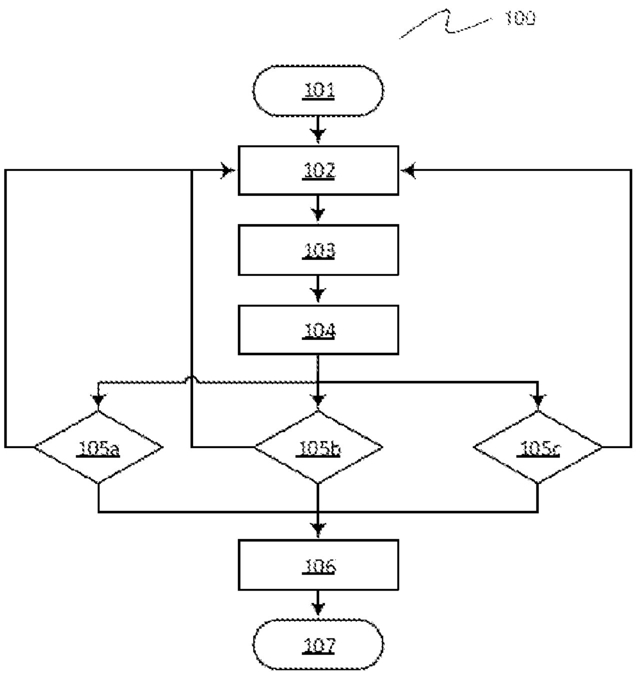
Norwegian Industrial Property Office

(21)	Application nr.	20171742	(86)	International Filing Date and Application Number	
(22)	Date of Filing	2017.11.02	(85)	Date of Entry into National Phase	
(24)	Date of Effect	2017.11.02	(30)	Priority	2017.09.15, US, 62/559,214
(41)	Publicly Available	2019.03.18			
(45)	Granted	2024.05.13			

(73)	Proprietor	ELLIPTIC LABORATORIES ASA, Hausmanns gate 21, 0182 OSLO, Norge
(72)	Inventor	Laila Danielsen, 424 Village drive, CA94530 EL CERRITO, USA Holger Hussmann, Kåres Vei 6 A, 1185 OSLO, Norge Guenael Thomas Strutt, 36 Bob Kaufman Alley, CA94133 SAN FRANCISCO, USA
(74)	Agent or Attorney	BRYN AARFLOT AS, Stortingsgata 8, 0161 OSLO, Norge

(54)	Title	**User Authentication Control**
(56)	References Cited:	CN 106778179 A, EP 3133474 A1, EP 3108406 A2, CN 106446801 A, CN 106709308 A, CN 107092820 A, US 2009318810 A1, CN 105869251 A
(57)	Abstract	

Present teachings relate to a method for initiating an authentication process on an electronic device, the method comprising transmitting an ultrasound signal from an ultrasound transmitter, generating a measured signal by receiving at an ultrasound receiver an echo of the ultrasound signal being reflected by an object, analyzing the echo by processing the measured signal, and initiating the authentication process on the electronic device based on the processing of the measured signal. The present teachings also relate to a method for maintaining an authenticated state of an object. The present teachings also relate to an electronic device comprising an ultrasound system for initiating an authenticating process. The present teaching also relate to an electronic device comprising an ultrasound system for retaining an authenticated state of an object. The present teachings also relate to computer software products for implementing any method steps disclosed herein.



USER AUTHENTICATION CONTROL

Technical Field

Present teachings relate to user recognition for an electronic device.

Background Art

A number of authentication technologies exist for authenticating a rightful user of an electronic device, including fingerprint sensing, iris scan, password or pin code, and facial recognition. When using most of these technologies there is a certain delay associated with the authenticating process. In addition to this, there might be delay associated with the start of the authenticating process. In fingerprint scanning system on a mobile device, for example, the user pressing the home button of the mobile device might be used to trigger the authenticating process. Such a process is discussed in CN106778179 where the authentication is triggered by a user request. In EP3133474 a solution is described where movements are used to trigger a gesture measurement, thus representing a complex system where the movements as such would not be suitable for authentication.

In facial recognition based authentication systems, especially those without a dedicated button, the mobile device must determine when to trigger the authentication process. Such a trigger may be a lift to wake function, or another process initiated by the user of the mobile device. Another option could be to activate the facial recognition system at regular intervals to detect a user, but this will lead to high power consumption of the device even if the intervals are infrequent. In addition, the triggering of the authentication process may be unreliable such that the user experience is affected. The authentication process is unreliable if the triggering system does not initiate the authentication process, even though the process should have been initiated. In such conditions the user may experience undesired delays in unlocking their device.

Summary

At least some problems inherent to the prior-art will be shown solved by the features of the accompanying independent claims.

Viewed from a first aspect a method for estimating the position and/or movement of an object is provided. In one embodiment, the present teachings can provide a method for initiating an authentication process on an electronic device, the method comprising transmitting an ultrasound signal from an ultrasound transmitter, generating a measured signal by receiving at an ultrasound receiver an echo of the ultrasound signal being reflected by an object, analyzing the echo by processing the measured signal, and initiating the authentication process on the electronic device based on the processing of the measured signal.

According to an embodiment, the method comprises computing a distance value by the processing of the measured signal, said distance value being relative to the distance between the object and the electronic device.

As will be appreciated, the transmitter and receiver may either be different components or alternatively can be the same transducer being used in a transmit mode for transmitting the ultrasound signal and then in a receive mode for receiving the reflected ultrasound signal. If the transmitter and receiver are different components, they may be placed in the same location, or they may be installed at different locations on the electronic device. Furthermore, the electronic device may comprise a plurality of transmitters and/or a plurality of receivers. Multiple transmitter-receiver combinations may be used to extract spatial information related to the object and/or surroundings.

The processing of the measured signal can be done by a processing unit such as a computer processor.

The electronic device may be any device, mobile or stationary, which is required to authenticate the user. Accordingly, devices such as mobile phones, smartwatches, tablets, notebook computers, desktop computers, and similar devices fall within the ambit of the term electronic device. In addition, devices such as vending machines, automobiles, gates, doors, home appliances, and other kinds of electronic access systems that require electronic authentication also fall within the ambit of the term.

In some cases, a hand of the user may be considered an object. Alternatively, if a user is considered an object, the hand may be considered as a part of the object. In other cases, the hand and the rest of the user's body may be considered different objects, given the range and/or sensitivity of the field of view of the ultrasound transmitter/receiver combination. The range and/or sensitivity may either be limited according to component specifications, or it may be statically or dynamically set to a certain values according to processing requirements.

The authentication process is preferably facial recognition system; however, the teachings may also be applied to other kinds of authentication processes.

According to an embodiment, the authentication process is initiated when the computed distance value is shorter than a distance threshold value. According to another embodiment, the method may also comprise estimating a movement of the object relative to the electronic device by transmitting a stream of ultrasound signals and by computing a trajectory of the object by combining the computed distance values associated with a stream of reflected ultrasound signals from the object. In other words, the stream or sequence of transmitted ultrasound signals results in a stream or sequence of ultrasound signals reflected from the object, for each reflected signal in the stream of ultrasound signals received by the receiver, a corresponding measured signal is generated, thereby resulting in a stream of measured signal values. The stream of measured signals can be used to estimate the trajectory of the object. The estimated trajectory may also be used to compute a projected trajectory of the object, the projected trajectory being a probabilistic estimate of the future movement of the object based upon the estimated trajectory. According to an embodiment, the initiation of the authentication process is done on the basis of the estimated trajectory and/or the projected trajectory of the object. In such case, the method may comprise computing of a confidence value. The confidence value can be related to the probability that the user is going to use the electronic device. The confidence value may be generated based upon one or more of the characteristics of the movement. The authentication process may be initiated if the confidence value is larger than a confidence value threshold.

The characteristics of the movement include the speed of the object, the direction of the object, and the size of the object. In some cases, different reflections may be received from different parts of the object. If the object is the user, the ultrasound receiver may receive reflections from different parts of the user's body, for example, the user's hand and the user's face. Accordingly, the method may comprise measuring the relative position and/or movement of the different parts of the object for computing the confidence value, or improving a previously computed confidence value. If required, the method can also comprise tracking the relative movements of different parts of the object.

According to another embodiment, the method comprises recognizing a movement gesture executed at least by a part of the object for initiating the authentication process. A predetermined gesture may be used by the user to wake up the device and/or to initiate the authentication process.

The threshold value may either be a fixed value, or it may be a dynamic value based upon the use case of the electronic device. Some non-limiting examples of the use cases threshold values are provided later in this disclosure.

According to another embodiment, the method also comprises transmitting data related to the object to another electronic module of the electronic device. The object related data may include one or more of: object position, distance, speed, estimated trajectory, and projected trajectory. Another electronic module may be a hardware or software module, and may include any one or more of, application programming interface ("API"), and sensor fusion module. For example, data related to either one or any of, distance, speed of movement, position, and gesture type may be transmitted to a facial recognition algorithm.

According to another embodiment, the method comprises receiving data from at least one of the other sensors or modules in the electronic device for improving the robustness of the initiation of the authentication process. The other sensors or modules may include, accelerometer, inertial sensor, IR sensor, or any other sensor or modules related to a sensor fusion module in the electronic device.

As will be appreciated, the method can be used for initiating the authentication process not only based upon a measurement of the reflected signal or echo from an object facing the screen of the electronic device, but also from an object that is located on a side of the electronic device. Accordingly, the method can provide for the initiation of the authentication process if the object approaches one of the sides of the electronic device. Hence, a wider sensitivity space is achieved for initiating the authentication process, which can save precious time for unlocking the electronic device. A smoother and more seamless user experience may thus be achieved.

According to another aspect of the present teachings, a method for maintaining an authenticated state of an object can be provided, the method comprises receiving a confirmation signal from an authentication module of an electronic device confirming that the object is a rightful user of the electronic device, initiating a tracking phase for tracking the object by using a stream of transmitted ultrasound signals transmitted from an ultrasound transmitter, analyzing a stream of echoes received by an ultrasound receiver, the stream of echoes being reflections of the stream of ultrasound signals analyzing the corresponding stream of echoes received by an ultrasound receiver, computing a probability value related to the object being the rightful user by analyzing the stream of echoes. The method further comprises preventing the electronic device from going into a locked state if the probability value is higher than a first probability threshold value. The probability value can be related to the distance of the object from the electronic device. Accordingly, if the object or user moves beyond a distance value threshold from the electronic device, the electronic device may enter a locked state requiring a user to authenticate before using the electronic device. According to yet another embodiment, if a plurality of objects or users are detected during the tracking, the probability value may be lowered based upon the certainty with which the tracking is able to distinguish the rightful user from the plurality of objects. The probability may also be lowered if a conflict is detected in the received echoes. According to yet another embodiment, the method comprises configuring the electronic device into the locked state if the probability value is lower than a second probability threshold. The first probability threshold and the second probability threshold may be either different values or a same value. It will be appreciated; having different first and second probability threshold values might be desirable for achieving hysteresis. The present teachings may therefore also enable on-body detection for mobile devices, where the mobile device may not be required to enter a locked state as long as the rightful user has once authenticated themself and has subsequently not left the vicinity of the mobile device. Such conditions might for example be, if the mobile device is in a pocket of the authenticated user.

The threshold values may either be static or they may be dynamic. Using dynamic values may be preferable based on the use. For example, a threshold value for a given parameter for on-body detection can be different from a threshold value for the same parameter in another mode. The distance threshold, for example, may range from a sub-centimeter to several meters. The range of detection is dependent on the component specifications and power consumption, so any distance values should not be considered limiting to the generality of the present teachings.

The processing of the echo signals may be based on time of flight (“TOF”) measurements between the transmitted ultrasound signal and the corresponding measured signal. The processing of the echo signals may also be based on the amplitude of the measured signal, or phase difference between the transmitted signal and the measured signal, or the frequency difference between the transmitted signal and the measured signal, or a combination thereof. The transmitted ultrasound signal may comprise either a single frequency or a plurality of frequencies. In another embodiment, the transmitted ultrasound signal may comprise chirps.

The method steps are preferably implemented using a computing unit such as a computer or a data processor.

Viewed from another aspect, the present teachings can also provide an electronic device implementing the embodiments discussed above. More specifically, an electronic device is provided, the electronic device comprising an ultrasound system adapted to initiate an authentication process on the electronic device, wherein the ultrasound system comprises

an ultrasound transmitter configured to transmit an ultrasound signal,

an ultrasound receiver configured to receive an echo of the ultrasound signal, the ultrasound receiver also being configured to generate a measured signal relative to the echo, and

a processing unit configured to analyze the echo by processing the measured signal, wherein

the processing unit is configured to initiate the authentication process on the electronic device based on the processing of the measured signal.

The processing unit can be any type of computer processor, such as a DSP, an FPGA, or an ASIC.

Viewed from another aspect, the present teachings can also provide an electronic device comprising an ultrasound system adapted to maintain an authenticated state on the electronic device, wherein the ultrasound system comprises

an ultrasound transmitter configured to transmit an ultrasound signal,

an ultrasound receiver configured to receive an echo of the ultrasound signal, the ultrasound receiver also being configured to generate a measured signal relative to the echo, and

a processing unit configured to analyze the echo by processing the measured signal, wherein

the processing unit is configured to retain the electronic device in the authenticated state based on the processing of the measured signal.

Viewed from yet another aspect, the present teachings can also provide a computer software product for implementing any method steps disclosed herein. Accordingly, the present teachings also relate to a computer readable program code having specific capabilities for executing any method steps herein disclosed.

Example embodiments are described hereinafter with reference to the accompanying drawings.

Brief description of drawings

FIG. 1 shows a flowchart illustrating a method for initiating an authentication process of an electronic device

FIG. 2 shows a flowchart illustrating a method for maintaining an authenticated state of an electronic device

Detailed description

FIG. 1 shows a flowchart 100 illustrating a method for initiating an authentication process on an electronic device. Upon start 101, as a first step 102, an ultrasound signal is transmitted by an ultrasound transmitter. In a following step 103, an echo signal of the ultrasound signal is received by an ultrasound receiver. If an object is present in the field of view of the ultrasound transmitter and receiver, the echo signal will comprise at least one echo reflected by the object. The ultrasound receiver generates a measured signal relative to the received echo signal. In a following step 104, the echo signal is analyzed by processing the measured signal. The processing is performed by a computer processor. During processing, the processor extracts parameters related to the object. The parameters include one or more of: distance, position, speed, direction, movement, or type or gesture performed by the object. One or more of said parameters are evaluated against predetermined thresholds or criteria associated with each of the evaluated parameters. This is shown as a plurality of steps 105. Three evaluations, 105a, 105b and 105c are shown in the figure, however the evaluations may be more or fewer than those shown. Furthermore, the evaluation steps may be performed concurrently or sequentially to each another. The evaluation steps may even be performed selectively, i.e., some evaluations may be performed according to requirement.

As an example, the first evaluation 105a could be comparing a distance value, computed by processing the measured signal, with a predetermined distance threshold value. Similarly, the second evaluation 105b could be comparing a speed value with a predetermined distance threshold value. Similarly, the third evaluation 105c could be comparing a movement pattern with a predetermined database of recognized gestures. It will be understood that for extracting parameters such as speed and movement, a plurality of ultrasound signals and echoes might be required. As a result, the transmitting of the ultrasound signal and receiving of echo includes both cases, i.e., a single pulse and a burst of pulses. The transmitted ultrasound signal might have different profiles, all of which are relevant to this disclosure. For example, the ultrasound signal may comprise chirps. Furthermore, the processing of the measured signal may include one or any of: time of flight measurements, phase shift measurements, amplitude measurements, or frequency shift measurements. The respective threshold values may be static of they may be dynamic. If the distance value is shorter than the predetermined distance threshold value, then in a following step 106, the authentication process is initiated. If, however, the distance value is larger than the predetermined distance threshold value, the method step102 is repeated, i.e., transmitting a new ultrasound signal using the transmitter. The new ultrasound signal may either be similar to the previously transmitted signal or it may be different, for example, dependent upon the processing of the measured signal. In cases for example, where ambient noise beyond a predetermined limit is detected during processing, the ultrasound signal may be altered to achieve a better signal to noise ratio in subsequent measurements. Whether the method step 106 of initiating the authentication process is executed, or the step 102 of transmitting the ultrasound signal is performed, may be decided either individually of any of the evaluation steps 150a-c or in combination, whichever provides a better confidence that the authentication process should be started. A series or stream of measurements either done within steps 102 – 104 or from steps 102 – 105 may also be used to compute one or more of the following: an estimated trajectory of the object, a projected trajectory of the object, measuring/tracking multiple objects, measuring/tracking relative movements of multiple objects or multiple parts of an object.

FIG. 2 shows a flowchart 200 illustrating a method for maintaining an authenticated state of an object. As a first step 201, a confirmation signal is received from an authentication module of an electronic device confirming that the object is a rightful user of the electronic device. In an optional following step 203, it can be checked if a locked state has been initiated by any other module, for example by the user themselves by pressing a button, or by another security module. If locked state is not initiated, in step 203, a stream of ultrasound signals is transmitted by an ultrasound transmitter. In a following step 204, a stream of echoes of the transmitted ultrasound signal is received by an ultrasound receiver. The echo stream is analyzed by a processor either as a part of the receiver or a separate module. As discussed previously, the receiver generates a measured signal relative to the echo stream, so the processor performs one or more analysis on the measured signal generated dependent upon the echo stream received by the ultrasound receiver. Based upon said one or more analysis of the measured signal, or echo stream, a probability value is computed, in step 206, by the processor or processing unit. The one or more analyses are shown as steps 205a – c. The probability value may be generated as a result of either one of the evaluation steps 205a – c, or any of their combinations. Three evaluation steps 205a – c are shown, however, the number of evaluation steps may be greater or less than three. The evaluation steps may be performed concurrently, sequentially, or selectively.

As an example, the first evaluation step 205a may be computing a distance of the object from the electronic device. The second evaluation step 205b may be detecting other objects in the field of view. The third evaluation step 205c may be movement of an object.

In a next step, 207, the probability value is compared with a first probability threshold value. If the probability value is higher than the first probability threshold value, there is enough confidence that the object is the authenticated user. In such case the steps 202 and following can be repeated for tracking the object and computing a new probability value. If, however, the probability value is lower than the first probability threshold value, the method as an optional step 209 may compare the probability value with a second probability threshold value. If the probability value is higher than the second probability threshold value, it may be assumed that there is still enough confidence that the object is the authenticated user. In such case, steps 202 – 207 can be repeated for tracking the object and computing a new probability value. If, however, the probability value is lower than the second probability threshold value, it is deemed that there is not enough certainty or confidence than an object detected is the authenticated user. In this case, as a following step 210, the electronic device is brought to a locked state such that user authentication must be performed to unlock the electronic device. In the end step 211, the method can either conclude, or initiate the method for initiating an authentication process as described previously.

The skilled person will appreciate that method and product embodiments discussed herein may be freely combined.

Claims

1.

A method for initiating an authentication process on an electronic device, the method comprising:

- transmitting a stream of ultrasound signals from an ultrasound transmitter;
- receiving at an ultrasound receiver echoes of the stream of ultrasound signals being reflected by an object;
- for each echo of an ultrasound signal being reflected by the object, generating a measured signal;
- analyzing each echo by processing the measured signal by computing a distance value, said distance value being related to the distance between the object and the electronic device;
- estimating the movement of the object by combining the computed distance values associated with the stream of reflected ultrasound signals from the object;
- calculating a confidence value based on one or more characteristics of the movement, wherein the confidence value is related to the probability that the user is going to use the electronic device, and
- initiating the authentication process on the electronic device when the confidence value is higher than a confidence value threshold.

2.

The method according to claim 1, wherein the authentication process is a facial recognition process

3.

The method according to claim 1, wherein the method further comprises computing a projected trajectory of the object.

4.

The method according to claim 1, wherein the authentication process is initiated when a movement gesture performed by the object is detected.

5.

An electronic device comprising an ultrasound system adapted to initiate an authentication process on the electronic device, wherein the ultrasound system comprises:

an ultrasound transmitter configured to transmit a stream of ultrasound signals,

an ultrasound receiver configured to receive a stream of echoes of the ultrasound signal reflected by an object;

the ultrasound receiver also being configured to generate a measured signal from each received echo, and

a processing unit configured to analyze each echo by processing the measured signal by computing a distance value , said distance value being related to the distance between the object and the electronic device,

the processing device also being configured to estimate the movement of the object by combining the computed distance values associated with the stream of reflected ultrasound signals from the object; and

the processing unit is also configured to calculate a confidence value based on one or more characteristics of the movement, wherein the confidence value is related to the probability that the user is going to use the electronic device, wherein the processing unit is configured to initiate the authentication process on the electronic device when the confidence value is higher than a confidence value threshold.

6.

A computer software product having specific capabilities for executing the steps of:

- transmitting an ultrasound signal from an ultrasound transmitter;
- receiving at an ultrasound receiver echoes of the stream of ultrasound signals being reflected by an object;
- for each echo of an ultrasound signal being reflected by the echo, generating a measured signal;
- analyzing each echo by processing the measured signal by computing a distance value, said distance value being related to the distance between the object and the electronic device;
- estimating the movement of the object by combining the computed distance values associated with the stream of reflected ultrasound signals from the object;
- calculating a confidence value based on sone or more characteristics of the movement, wherein the confidence value is related to the probability that the user is going to use the electronic device and the distance from the device; and
- initiating the authentication process on the electronic device when the confidence value is higher than a confidence value threshold.

Patentkrav

1.

Fremgangsmåte for initiering av en autentifiseringsprosess på en elektronisk innretning, der fremgangsmåten omfatter:

- sending av en strøm av ultralydsignaler fra en ultralydsender;
- mottak ved en ultralyd-mottaker, ekko av en strøm av ultralydsignaler reflektert av et objekt;
- for hvert ekko av et ultralydsignal reflektert av objektet, generere et målesignal;
- analysering av hvert ekko ved prosessering av det målte signalet ved å beregne en avstandsverdi, der avstandsverdien er relatert til avstanden mellom objektet og den elektroniske innretningen;
- estimering av objektets bevegelse ved kombinering av beregnede avstandsverdier assosiert med strømmen av reflekterte ultralydsignaler fra objektet;
- beregning av en konfidensverdi basert på en eller flere egenskaper ved bevegelsen, hvori konfidensverdien er relatert til sannsynligehten for at brukeren kommer til å bruke den elektroniske enheten, og
- initiering av autensifiseringsprosessen på den elektroniske enheten dersom konfidensverdien er høyere enn en terskeverdi for konfidensverdien.

2.

Fremgangsmåte ifølge krav 1, hvori autentifiseringsprosessen er en ansiktsgjenkjenningsprosess.

3.

Fremgangsmåte ifølge krav 1, hvori fremgangsmåten videre omfatter beregning av en projisert bane for objektet.

4.

Fremgangsmåte ifølge krav 1, hvori autentifiseringsprosessen er initiert når en bevegelses-gest utført av objektet er detektert.

5.

Elektronisk innretning omfattende et ultralydsystem innrettet itl å initiere en autentifiseringsprosess på en elektronisk innretning, der ultralydsystemet omfatter:

en ultralydsender konfigurert til å sende en strøm av ultralydsignaler

en ultralydmottaker konfigurert til å motta en strøm av ekkoer av ultralydsignalet reflektert fra et objekt,

der ultralydmottakeren også er konfigurert til å generere et målesignal for hvert mottatt ekko, og

en prosesseringsenhet konfigurert til å analysere hvert ekko ved prosessering av det målte signalet ved beregning av en avstandsverdi, der avstandsverdien er relatert til avstanden mellom objektet og den elektroniske innretningen,

der prosesseringsenheten også er konfigurert til å estimere bevegelsen til objektet ved å kombinere de beregnede avstandsverdiene assosiert med strømmen av reflekterte ultralydsignaler fra objektet, og

prosesseringsenheten også er konfigurert til å beregne en konfidensverdi basert på en eller flere egenskaper ved bevegelsen, hvori konfidensverdien er relatert til sannsynligheten for at brukeren kommer til å bruke den elektroniske innretningen,

hvori prosesseringsenheten er konfigurert til å initiere autentifiseringsprosessen når konfidensverdien er høyere enn en konfidensverdi terskelverdi.

6.

Et programvareprodukt for en datamaskin med spesifikke egenskaper for utføring av følgende trinn:

- sending av en strøm av ultralydsignaler fra en ultralydsender;
- mottak ved en ultralyd-mottaker, ekko av en strøm av ultralydsignaler reflektert av et objekt;
- for hvert ekko av et ultralydsignal reflektert av objektet, generere et målesignal;
- analysering av hvert ekko ved prosessering av det målte signalet ved å beregne en avstandsverdi, der avstandsverdien er relatert til avstanden mellom objektet og den elektroniske innretningen;
- estimering av objektets bevegelse ved kombinering av beregnede avstandsverdier assosiert med strømmen av reflekterte ultralydsignaler fra objektet;
- beregning av en konfidensverdi basert på en eller flere egenskaper ved bevegelsen, hvori konfidensverdien er relatert til sannsynligheten for at brukeren kommer til å bruke den elektroniske enheten og avstanden fra enheten, og
- initiering av autentifiseringsprosessen på den elektroniske enheten dersom konfidensverdien er høyere enn en terskelverdi for konfidensverdien.

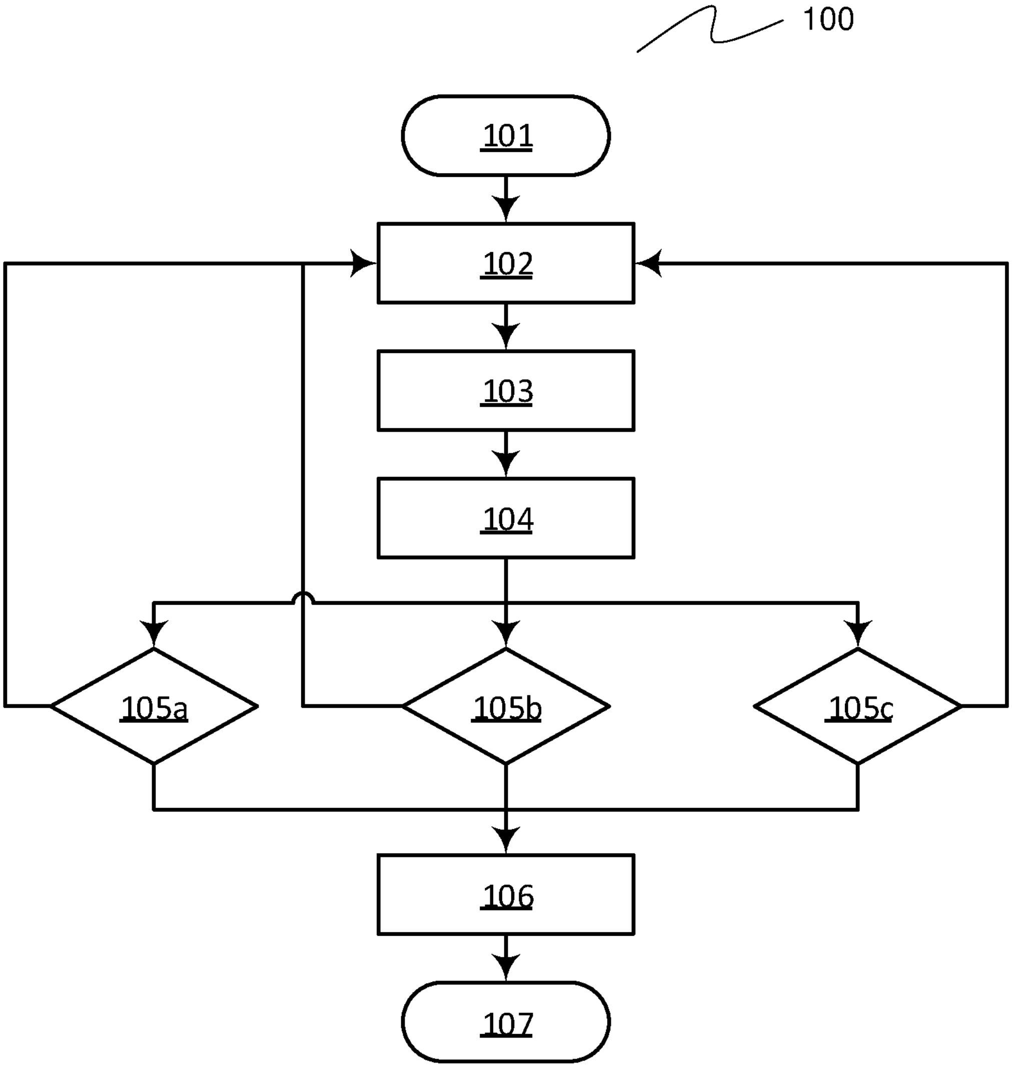


FIG. 1

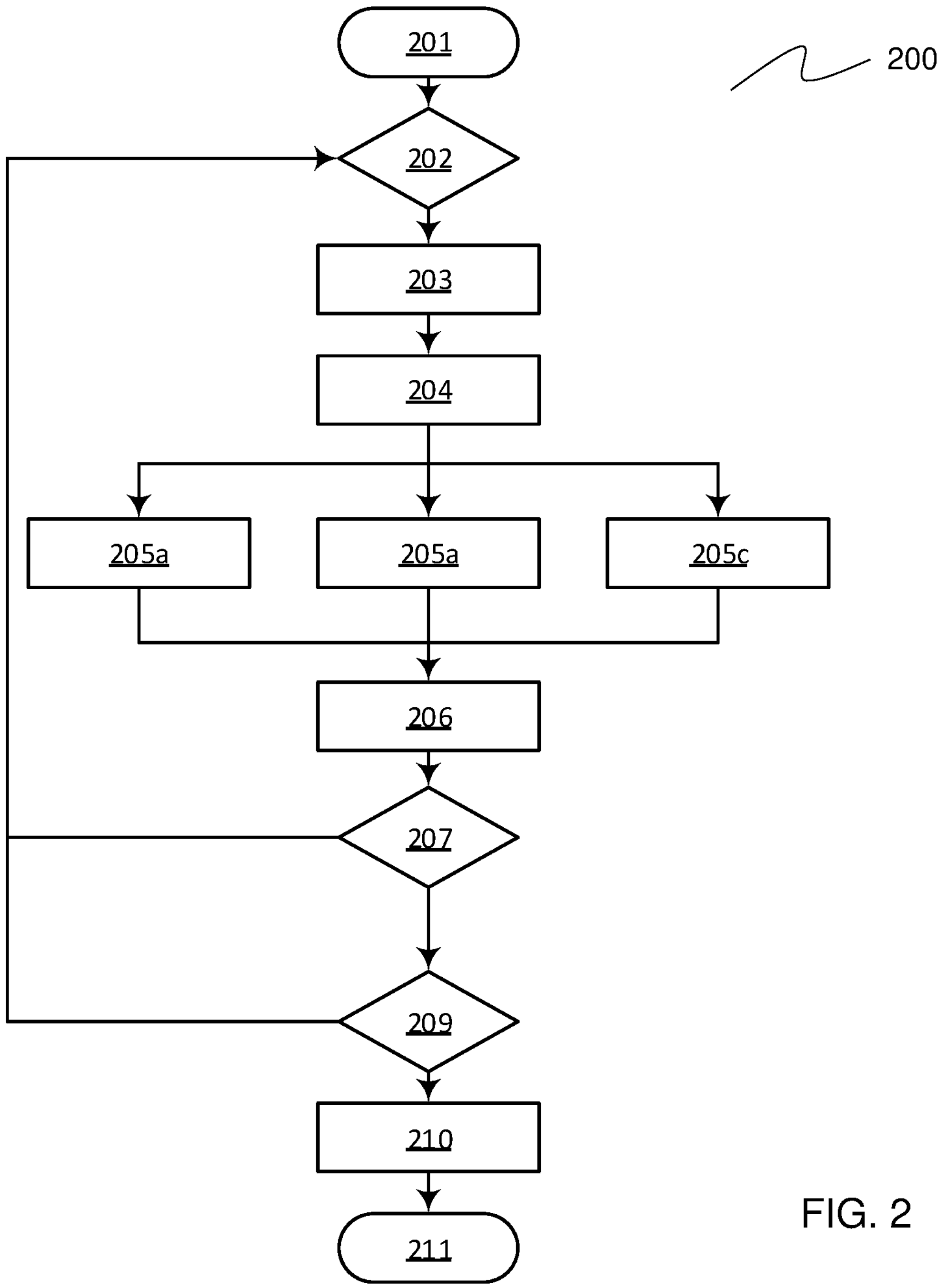


FIG. 2