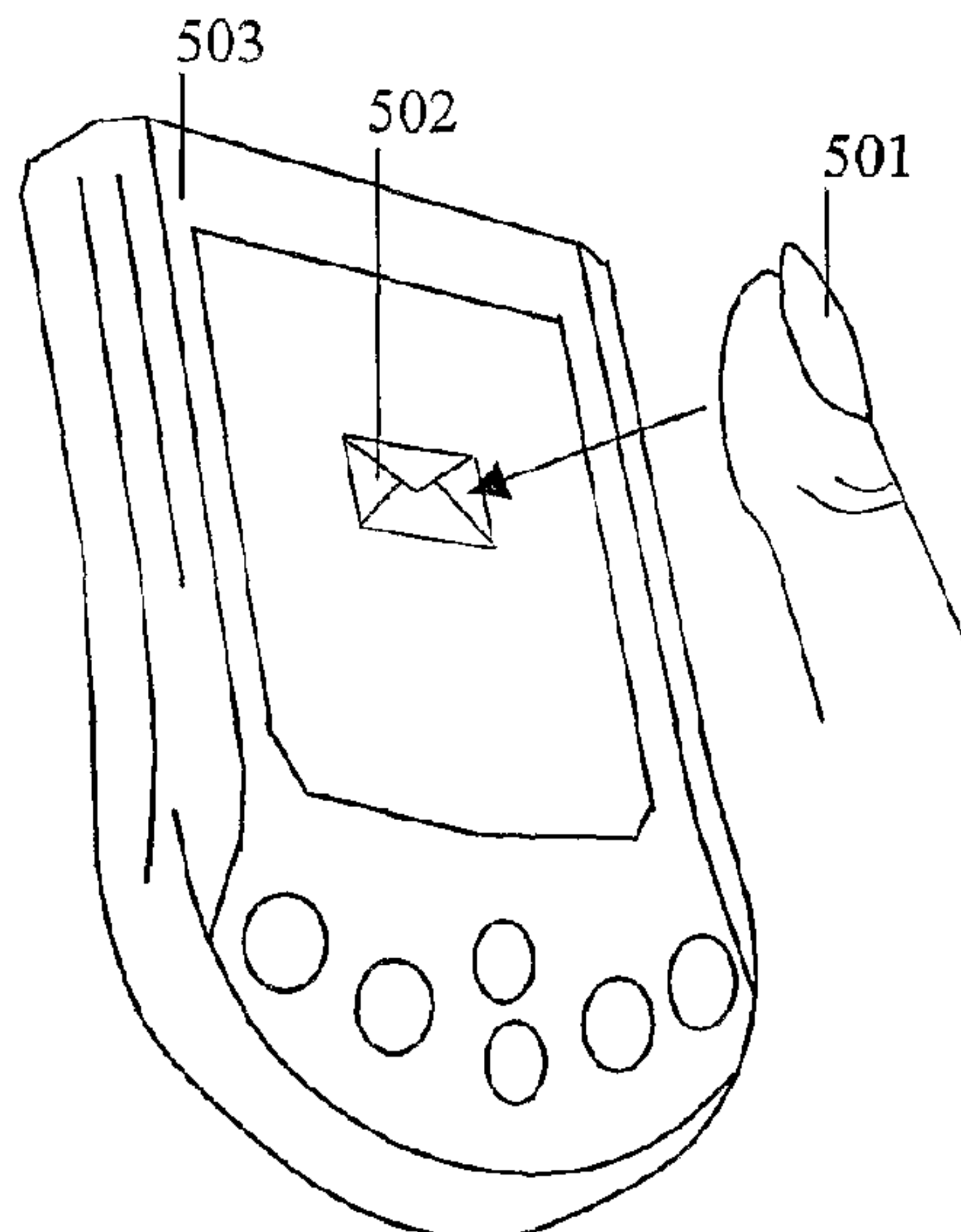




(86) **Date de dépôt PCT/PCT Filing Date:** 2004/06/01
 (87) **Date publication PCT/PCT Publication Date:** 2004/12/16
 (45) **Date de délivrance/Issue Date:** 2016/09/27
 (85) **Entrée phase nationale/National Entry:** 2005/11/30
 (86) **N° demande PCT/PCT Application No.:** US 2004/017270
 (87) **N° publication PCT/PCT Publication No.:** 2004/109454
 (30) **Priorité/Priority:** 2003/05/30 (US60/474,750)

(51) **Cl.Int./Int.Cl. G09G 5/00** (2006.01)
 (72) **Inventeurs/Inventors:**
 ABDALLAH, DAVID S., US;
 JOHNSON, BARRY W., US;
 OLVERA, KRISTEN R., US
 (73) **Propriétaire/Owner:**
 APPLE INC., US
 (74) **Agent:** RICHES, MCKENZIE & HERBERT LLP

(54) **Titre : INTERFACE HOMME-MACHINE DE COMMANDE D'ACCES A DES DISPOSITIFS ELECTRONIQUES**
 (54) **Title: A MAN-MACHINE INTERFACE FOR CONTROLLING ACCESS TO ELECTRONIC DEVICES**



(57) **Abrégé/Abstract:**

The invention disclosed herein describes a man-machine interface device (100) for controlling access to electronic devices. The man-machine interface device comprises an electronic display unit (102) including a transparent finger touch sensor region (101) that is seated above the display apparatus, which is responsible for determining the presence and absence of a finger and for generating fingerprint images when a finger is detected. The man-machine interface device also includes a controller unit (103) that is coupled to the display apparatus, the finger touch sensor region, and at least one electronic device. The method of the invention describes a process for authenticating individuals and verifying their security privileges to access sensitive data, based on a finger-touch selection of an icon presented on the display apparatus of the man-machine interface device.

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

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
16 December 2004 (16.12.2004)

PCT

(10) International Publication Number
WO 2004/109454 A3

- (51) International Patent Classification⁷: **G09G 5/00**
- (21) International Application Number:
PCT/US2004/017270
- (22) International Filing Date: 1 June 2004 (01.06.2004)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/474,750 30 May 2003 (30.05.2003) US
- (71) Applicant (for all designated States except US): **PRI-VARIS, INC.** [US/US]; 675 Peter Jefferson Parkway, Suite 150, Charlottesville, VA 22911 (US).
- (72) Inventors: **ABDALLAH, David, S.**; 1295 Swan Lake Drive #102, Charlottesville, VA 22902 (US). **JOHNSON, Barry, W.**; 1413 Teakwood Cove, Charlottesville, VA 22911 (US). **OLVERA, Kristen, R.**; 1642 Center Avenue, Charlottesville, VA 22903 (US).
- (74) Agents: **CHASTEEN, Kimberly, A.** et al.; Williams Mullen, 1 Old Oyster Point Road, Suite 210, Newport News, VA 23602 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- Published:**
- with international search report
 - before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments
- (88) Date of publication of the international search report:
27 January 2005
- For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A MAN-MACHINE INTERFACE FOR CONTROLLING ACCESS TO ELECTRONIC DEVICES

(57) Abstract: The invention disclosed herein describes a man-machine interface device (100) for controlling access to electronic devices. The man-machine interface device comprises an electronic display unit (102) including a transparent finger touch sensor region (101) that is seated above the display apparatus, which is responsible for determining the presence and absence of a finger and for generating fingerprint images when a finger is detected. The man-machine interface device also includes a controller unit (103) that is coupled to the display apparatus, the finger touch sensor region, and at least one electronic device. The method of the invention describes a process for authenticating individuals and verifying their security privileges to access sensitive data, based on a finger-touch selection of an icon presented on the display apparatus of the man-machine interface device.

WO 2004/109454 A3

WO 2004/109454

PCT/US2004/017270

TITLE

A Man-Machine Interface for Controlling Access to Electronic Devices

RELATED U.S. APPLICATION DATA

[01]

BACKGROUND OF THE INVENTION

Field of the Invention:

[02] This invention relates generally to the field of electronic device user interfaces and authorization techniques, and more specifically to the field of fingerprint imaging sensors and touch screen display apparatuses.

Necessity of the Invention:

[03] Modern electronic devices have developed a myriad of functionalities and associated user interfaces. Many electronic devices use a display screen, such as a monitor or display apparatus, to provide feedback to the user. Handheld devices, such as the personal digital assistant and the cell phone, have an important user interface constraint – form factor. In both devices, manufacturers desire to minimize the size and weight of the device; as one means to accomplish this, the display is small and buttons are placed close together.

[04] In recent years, manufacturers of many electronic devices have substituted touch screen technology for the traditional display. Touch screens have the same appearance and style of a traditional screen, but have the added ability to determine the location of applied pressure. This allows individuals to use a stylus in a similar manner as a person uses a mouse to point to icons on a monitor – the individual may touch the screen at the location of a

particular icon. Software running on the device determines the location of the touch and determines the associated software function, such as opening an address book. Because the additional button control interface can be eliminated, manufacturers can make the display larger and simpler to use.

[05] As the functionality of electronic devices expands, individuals may wish to protect certain data stored within the device. For example, the owner of a personal digital assistant may choose to use his PDA to send and receive private e-mail. If the data is particularly sensitive, a simple password or PIN combination may not be considered adequate security and the individual may desire to use biometric authentication on the device. The most common form of biometric authentication, fingerprint scanning, requires a hardware module that is typically the size of a postage stamp. On a device where size and weight are limited, the addition of this module can be costly.

Digital Fingerprint Capture Technologies:

[06] There are three common types of fingerprint capture technologies: optical, capacitive, and ultrasonic. Each of the three technologies combines its associated hardware capture mechanism, which varies from type to type, and typically a software or firmware controller. This controller is often responsible for analyzing the captured image, extracting minutia points, and creating a final template. Minutiae are points that represent all of the unique characteristics of a fingerprint – one example is the location of an intersection of ridges or valleys in the print. A template is typically composed of thirty minutiae and can be used to uniquely identify a fingerprint. This allows the scanner or other storage device to store only the requisite data points without storing the entire image.

[07] Of the three types of fingerprint capture technologies, optical scanners are the oldest and most common, and they are composed of a glass or plastic plate with a light source and a charge coupled device (CCD) beneath. The light source is typically an array of light emitting

diodes (LEDs), and the CCD is an array of light-sensitive diodes. When the finger is placed on top of the plate, the LEDs illuminate the finger and each diode of the CCD records the light that touched it, creating an image in which the ridges are dark and the valleys are light. Optical scanners are fairly resistant to temperature fluctuations, and can provide an image quality of approximately 500 dots per inch (dpi). One major concern of this technology is that latent prints – “left over” fingerprints on the plate – can cause a superpositioning effect and create error. Additionally, these types of scanners are susceptible to “gummi bear attacks”, in which a fingerprint is lifted from a glass or other object, placed on a pliable and sticky material, such as a gummi bear, and can provide a false acceptance. One other point of note is that the plate must be quite large; this creates ease of use but may take unavailable real estate on a board.

[08] Capacitive sensors are much newer than optical scanners, and are composed of an array of cells; each cell has two adjacent conductor plates, which are embedded within an insulating layer. The insulating layer is typically a glass plate. When the finger is placed on top of the insulating layer, it creates a subsequent electric field between the finger and the conductor plates, creating capacitance. Because the surface of a finger is a succession of ridges and valleys, the electric field varies over the face of the finger as the distance from the plate to the finger varies. The capacitance or voltage may be determined from the electric field, and is commonly translated into an 8-bit grayscale image with approximately 200 to 300 grid points in both the x- and y- plane. This creates more detailed data than the optical sensor. Capacitive scanners are typically smaller than optical sensors because the cells are composed of semiconductor devices, rather than a CCD unit.

[09] While capacitive scanners are cheaper and smaller than optical sensors, their durability is unknown due to their short time in use, and the small size can make it more difficult for an individual to enroll and authenticate properly. Most fingerprint sensors use

direct current (DC) coupling, although a few companies are beginning to use alternating current (AC) coupling to penetrate to the live layer of the skin. Because the capacitive scanner is dependent on the electric field and capacitance between a finger and the glass plate, the scanner cannot be fooled by the “gummi bear attack” as described above; the dielectric constant for the finger is much different from a gummi bear, and so the capacitance will vary significantly.

[10] The most accurate but least common finger-scanning technology is ultrasound imaging. In this type of sensor, two transducers are placed on the x- and y- axes of a plate of glass – one each for receiving and transmitting – for propagating ultrasound waves through a glass plate; when the finger is placed on top of the glass, the finger impedes the waves and the receiving transducer can measure the alteration in wave patterns. This type of scanner is very new and largely untested in a variety of conditions, but initial results show promise for the technology. It combines the large plate size and ease of use of the optical scanners with the ability to pervade dirt and residue on the scanner, an advantage of capacitive scanners.

Touch Screen Technologies:

[11] Touch screens are quite similar to the fingerprint scanners described above. They recognize a finger pressure on the screen and typically calculate the center or peak point of the pressure. Current touch screen technologies fall under five different types of technology: analog resistive, capacitive, infrared, acoustic wave, and near field imaging. The analog resistive, capacitive and acoustic wave technologies are the most commonplace due to their clarity and endurance under a variety of conditions. Infrared is very sensitive to a light touch and may be impractical, while near field imaging is very new, suitable for very harsh conditions, and frequently cost-prohibitive. For these reasons only the first three technologies are examined in much detail. Similarly to the fingerprint scanning technology

there is typically an associated software or firmware controller to perform requisite data analysis.

[12] The analog resistive technology is composed of a glass plate and a plastic plate stacked over a flat-panel screen or display. Both the glass and plastic plates are coated with a transparent conductive material, such that the conductive material is sandwiched between the two plates. Tiny separator dots keep the two plates from touching under normal conditions, but when pressure is applied to the plastic plate, the dots move and the two surfaces come together to conduct electricity. An electronic controller instantly calculates the x- and y-coordinates, allowing resistive touch screen technologies to have very high precision and resolution. This also allows an individual to have relative freedom when selecting an object as a stylus; the individual may use a pen, finger, or other convenient utility.

[13] Capacitive coupled technologies require the use of a conductive stylus – this may be a finger, but not a gloved hand because the cloth will prevent the conduction of charge.

Capacitive technologies use a flat-panel display with a single glass plate resting on top. The glass plate is covered in a transparent metal oxide on the exterior surface; when the finger or alternate stylus comes into contact with the conductive surface; capacitive coupling occurs at the point of contact and draws electrical current. The controller registers the change in current and the x- and y- coordinates can be determined. As mentioned above, because the technology requires use of a conductive stylus, non-conductive surfaces will prevent the change in electrical current and will not have any effect on the touch screen. Furthermore, the exposed glass surface in this technology makes it susceptible to scratches and can inhibit correct operation of the screen.

[14] Acoustic wave touch screens are more complicated than the capacitive and resistive technologies. There are two types of acoustic wave technologies: guided acoustic wave (GAW) and surface acoustic wave (SAW). Both use a single plate of glass placed on top of a

flat-panel display, with a similar transducer arrangement as described above for the ultrasound imaging. GAW screens transmit a wave through the glass panel (using the glass as a waveguide), while SAW screens transmit the wave on the surface of the glass; in both technologies, transducers detect a dampening of the wave that occurs when pressure is applied to the glass, which is translated into x- and y- coordinates. Similarly to the capacitive coupled screens, SAW screens have stylus limitations; the stylus must be soft and able to absorb energy in order to dampen the wave, and are generally only practical in instances where the stylus is a finger. These types of touch screens also have the glass surface limitation described above.

Description of the Related Art:

[15] A multitude of single-purpose display apparatuses, fingerprint sensors and touch screens are available commercially. Furthermore, several companies offer commercial products that embed fingerprint-scanning hardware within display apparatus technology. One such example, Ethentica and Philips FDS^{*} (a wholly owned subsidiary of Philips Corporation) joint venture TactileSense™ finger scanning hardware, comprises a transparent optical sensor that can be embedded into a pane of glass. The TactileSense optical sensor comprises several a unique TactileSense polymer, a silicon glass camera/CCD, and a control ASIC. The TactileSense polymer is placed on top of the silicon camera, which is embedded within glass to provide hardness and durability. The TactileSense polymer is the heart of the sensor, comprising five layers: insulating, black-coat, transparent conductive, light-emitting phosphor, and base. The insulating and black-coat layers enhance the performance of the sensor by preventing liquid or other particles from entering the sensor, and by preventing sunlight from entering the sensor. The chief layers are the transparent conductive and light-emitting phosphor layers, which serve to supply current to the polymer and to illuminate the fingerprint. When a finger is placed on the TactileSense polymer, the polymer illuminates

*** Trademark**

the fingerprint and creates an image. The silicon camera detects the illumination, and the ASIC converts it to digital format for processing.

[16] U.S. Pat. No. 6,327,376 to Harkin describes a fingerprint sensor comprised of an array of sensing elements. The sensing elements use both capacitive and optical techniques to generate the image; the device is constructed using a transparent conductive material for the electrodes contained within. However, despite the inclusion of the sensor within a display apparatus, there is little discussion of using the display as a touch screen or user navigation interface.

[17] U.S. Pat. No. 6,501,846 to Dickinson et al. discloses a method and system for computer access and cursor control using a relief object image generator. The relief object image generator is capable of capturing a 2-D image based on the 3-D relief of an object, such as a finger. The apparatus of Dickinson's invention can be used to simultaneously authenticate an individual's fingerprint, and move a cursor on a screen or perform other control-related functions related to the movement of the individual's finger. This application is targeted primarily at replacing mice, function keys, and other control mechanisms on devices where space is limited. However, Dickinson does not address use of biometric recognition incorporated with touch screen user navigation.

[18] DigitalPersona^{*} also offers fingerprint-scanning hardware that is transparent and can be placed over display apparatuses, marketed as U.are.U Crystal™. This hardware is also comprised of an optical sensor that uses completely transparent materials. It is ultra-thin, enabling it to be placed in mobile or other electronic devices where real estate is a significant concern. Again, however, this product does not demonstrate any of the touch screen properties as exhibited in the current invention.

* Trademark

BRIEF SUMMARY OF THE INVENTION

[19] The invention disclosed herein describes a man- machine interface device for controlling access to electronic devices. The man-machine interface device comprises an electronic display apparatus that is capable of presenting graphic text, images, icons, and other data typically shown on a screen, while further including a transparent finger touch sensor region that is seated above the display apparatus. This finger touch sensor region is responsible for determining the presence and absence of a finger, and is further responsible for generating fingerprint images when a finger is detected. The man-machine interface device also includes a controller unit that is coupled to the display apparatus, the finger touch sensor region, and at least one electronic device. The controller unit is capable of controlling data flow between the display apparatus, the finger touch sensor region and the electronic device, and for calculating finger touch locations based on a fingerprint image generated by the transparent finger touch sensor region. It can receive text from the electronic device, which is intended for presentation on the display apparatus, or conversely send a fingerprint image to the electronic device, among other functions.

[19a] Accordingly, in a further aspect, the present invention provides a non-transitory computer-readable storage medium storing one or more programs comprising instructions, which when executed by an electronic device with a touch screen display, cause the device to: display a plurality of icons on the touch screen display; detect, with the touch screen display, a finger touch event, by a user, at a touch location on the touch screen display that corresponds to a location of a respective icon from the plurality of icons displayed on the touch screen display, wherein the respective icon is associated with a respective function; and in response to detecting the finger touch event at the touch location on the touch screen display: in accordance with a determination that the

8a

respective function does not require fingerprint authentication, authorize the respective function; and in accordance with a determination that the respective function requires fingerprint authentication: determine a plurality of security privileges of the user based on a comparison between a fingerprint detected during the finger touch event and previously stored fingerprint information; and after determining the plurality of security privileges of the user, authorize the respective function when the plurality of security privileges of the user include a respective security privilege that indicates that the respective function is accessible to the user, wherein the plurality of security privileges of the user comprise a security privilege that indicates whether the user can access an electronic message that is received by the device from an external device.

[19b] In a still further aspect, the present invention provides an electronic device, comprising: a touch screen display; one or more processors; memory; and one or more programs, wherein the one or more programs are stored in the memory and configured to be executed by the one or more processors, the one or more programs including instructions for: displaying a plurality of icons on the touch screen display; detecting, with the touch screen display, a finger touch event, by a user, at a touch location on the touch screen display that corresponds to a location of a respective icon from the plurality of icons displayed on the touch screen display, wherein the respective icon is associated with a respective function; and in response to detecting the finger touch event at the touch location on the touch screen display: in accordance with a determination that the respective function does not require fingerprint authentication, authorizing the respective function; and in accordance with a determination that the respective function requires fingerprint authentication: determine a plurality of security privileges of the user based on a comparison between a fingerprint detected during the finger touch event and previously stored fingerprint information; and after determining the plurality of security

8b

privileges of the user, authorizing the respective function when the plurality of security privileges of the user include a respective security privilege that indicates that the respective function is accessible to the user, wherein the plurality of security privileges of the user comprise a security privilege that indicates whether the user can access an electronic message that is received by the device from an external device.

[19c] In a further aspect, the present invention provides a method, comprising: at an electronic device with a touch screen display: displaying a plurality of icons on the touch screen display; detecting, with the touch screen display, a finger touch event, by a user, at a touch location on the touch screen display that corresponds to a location of a respective icon from the plurality of icons displayed on the touch screen display, wherein the respective icon is associated with a respective function; and in response to detecting the finger touch event at the touch location on the touch screen display: in accordance with a determination that the respective function does not require fingerprint authentication, authorizing the respective function; and in accordance with a determination that the respective function requires fingerprint authentication: determine a plurality of security privileges of the user based on a comparison between a fingerprint detected during the finger touch event and previously stored fingerprint information; and after determining the plurality of security privileges of the user, authorizing the respective function when the plurality of security privileges of the user include a respective security privilege that indicates that the respective function is accessible to the user, wherein the plurality of security privileges of the user comprise a security privilege that indicates whether the user can access an electronic message that is received by the device from an external device.

[20] The method of the invention describes a process for authenticating individuals and verifying their security privileges to access sensitive data, based on a finger-touch

8c

selection of an icon presented on the display apparatus of the man-machine interface device.

BRIEF DESCRIPTION OF DRAWINGS

Master Reference Numeral List

Figure 1: Apparatus

100	Apparatus
101	Finger touch sensor region
102	Display apparatus
103	Controller

Figure 2: Apparatus, based on optical sensor technology

- 102 Display apparatus
- 201 Charge coupled device
- 202 Glass or plastic plate
- 203 Light source

Figure 3: Apparatus, based on capacitive sensor technology

- 102 Display apparatus
- 302 Glass plate, coated with transparent metal oxide
- 303 Electric field

Figure 4: Apparatus, based on ultrasonic/acoustic wave technology

- 102 Display apparatus
- 402 Glass plate
- 403 Ultrasonic/acoustic wave generator

Figure 5: Authenticating to the apparatus

- 501 Human thumb
- 502 E-mail icon
- 503 PDA

Figure 6: Method for authenticating

- 601 Is there a finger present?
- 602 Create a fingerprint image
- 603 Calculate the location of the finger touch
- 604 Is there an icon at the finger touch location?
- 605 Is there a function associated with the icon?
- 606 Does the function require fingerprint authentication?
- 607 Does the fingerprint match a stored fingerprint?
- 608 Determine access rights for matched fingerprint
- 609 Allow user access to function?
- 610 Authorize user access to function
- 611 Quit

[21] FIG. 1 is a schematic view of the apparatus of the invention.

[22] FIG. 2 is a schematic view of the apparatus of the invention, when optical sensing technology is used.

[23] FIG. 3 is a schematic view of the apparatus of the invention, when capacitive sensing technology is used.

[24] FIG. 4 is a schematic view of the apparatus of the invention, when ultrasonic/acoustic wave technology is used.

[25] FIG. 5 is a schematic view of the apparatus of the invention being used to authenticate to a PDA.

[26] FIG. 6 is a flow chart of the method of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[27] The apparatus of the invention is a primary man-machine interface device that incorporates biometric authentication into a touch-sensitive display. Juxtaposing these two technologies provides a simple user interface, and additionally, an economy of space for handheld or portable devices that require ease-of-use along with biometric authentication; devices can use the functionality of a display, control keys or buttons, and a fingerprint sensor, by replacing them with the man-machine interface device of this invention.

[28] Fingerprint scanning typically requires more detail, precision, and data analysis than touch screen technology. The most common use of fingerprint scanning is comparison between a new, "live" fingerprint, and an older stored fingerprint, where the comparison is typically between minutiae points calculated for both fingerprints. This can be used to verify or identify an individual who has already been entered into a system. If the fingerprint scanner fails to accurately analyze a print, the scanner may provide a false acceptance – reporting that the new fingerprint is the same as the old, when they actually are not – or false rejection – reporting that the two fingerprints are different when they are not. However, if a touch screen registers a touch location incorrectly, it is only a minor inconvenience to recalibrate the touch screen and renavigate the user interface.

[29] The primary embodiment of the man-machine interface device 100 incorporates a transparent finger touch sensor region 101, an electronic display apparatus 102, and a controller 103, as seen in Figure 1. The finger touch sensor region 101 is layered on top of the display apparatus 102, and is capable of determining the presence and absence of finger touches. It can additionally generate fingerprint images, which are transmitted to, and used

by, the controller 103. The display apparatus 102 must be capable of presenting graphic data, text, images, icons and other information, and may range from a cathode ray tube display, such as a television or monitor, to a liquid crystal display. The controller 103 is coupled to the finger touch sensor region 101 and the display apparatus 102, as well as peripheral electronic devices, such as a PDA.

[30] One alternate embodiment of the apparatus 100 is based on optical fingerprint scanner technology, and can be seen in Figure 2. A plate 202 is placed over the display apparatus 102, with a light source 203 and a CCD 201 between the two. The light source 203, the plate 202, and the CCD 201 must all be transparent, or items would not be viewable on the display apparatus 102.

[31] Figure 3 shows an alternate embodiment of the present invention, which is based on a capacitive fingerprint sensor and a capacitive touch screen. A glass plate 302 coated with transparent metal oxide is placed on top of the display apparatus 102. When the finger is placed on the glass plate of the finger touch sensor region 101, an electric field 303 is created and the finger touch location and fingerprint can be determined.

[32] Another alternate embodiment of the apparatus 100 is based on the ultrasonic imaging fingerprint sensor and the acoustic wave touch screen. This can be seen in Figure 4. Again a glass panel 402 is placed on the display apparatus 102. Ultrasonic waves 405 are propagated by means of an ultrasonic or acoustic wave generator 403 either through or on top of the glass panel 402, using it as a wave guide. When a finger is placed on the finger touch sensor region 101 it interferes with the traveling wave, generating the fingerprint or touch location. Because the wave guide is based on the principle of total internal reflection, the angle of incidence of the propagating wave 405 must be such that it doesn't interfere with the optical properties of the display apparatus 102 behind it. This is affected by the thickness of the glass panel 402 and the frequency of the propagating wave 405.

[33] Regardless of the embodiment of the apparatus 100, the controller 103 must be capable of receiving data from a peripherally-connected electronic device and displaying it on the display apparatus 102. The controller 103 must also be able to receive fingerprint images from the finger touch sensor region 101, and to calculate the location of finger touch events from these images. Additionally, the controller 103 is responsible for calculating minutiae points of a fingerprint associated with a finger touch on the finger touch sensor region 101. Any calculated data, such as a location or minutiae, can be transmitted from the controller 103 back to the peripheral device. If required, the controller 103 may be capable of storing fingerprint minutiae points, and/or comparing fingerprint minutiae points. In one preferred embodiment of the invention, the location can be determined by extrapolating the center point of the finger touch on the finger touch sensor region 101. However, the algorithmic choice does not fall within the scope of this invention; the location can be determined by any appropriate method.

[34] The peripherally-connected electronic device referred to above is the device using the man-machine interface device. For example, if the man-machine interface device were to be used as a replacement for the touch screen and buttons on a personal digital assistant (PDA), the PDA would be considered the peripherally-connected electronic device. It is responsible for sending data to the controller 103 for display on the display apparatus 102, and for requesting and receiving finger touch data. Additionally, the peripherally-connected electronic device is responsible for maintaining the association between icons or text pictured on the display apparatus 102, and accessing rights for said functions.

[35] The method of the invention provides fingerprint authentication for functions represented by an icon on a display. In the primary embodiment, the method is employed while using the man-machine interface device 100 installed in a PDA, but can be used with other suitable technology; examples explained herein will employ both. The method is

intended to replace traditional user interface and authentication methods. For example, the PDA may receive e-mail, which the intended recipient wishes to keep secure. The PDA stores a registered fingerprint for the intended recipient that is associated with the security privileges of the e-mail program. Additionally, the PDA displays an icon on the display apparatus 102 that accesses the e-mail program on selection.

[36] Figure 5 shows an individual 501 using the man-machine interface device 100 of the present invention, to touch the finger touch sensor region 101 over the icon 502 displayed on the display apparatus 102 of the PDA 503 – in this example, the e-mail icon. As seen in the flow chart of Figure 6, the finger touch sensor region 101 detects the presence of the finger (step 601), and generates an image of the fingerprint (step 602), which is passed to the controller 103. The controller 103 calculates the finger touch location (step 603), and determines if there is an icon displayed on the display apparatus 102 at that location (step 604). If an icon exists, the PDA determines which function is associated with the icon (step 605) and if the function requires fingerprint authentication (step 606).

[37] If the function does not require authentication, the PDA directly authorizes access to the function. However, in this example with e-mail, the function does require fingerprint authentication. The PDA examines stored fingerprints, verifying the new image against the stored images (step 607), until a match is found. If a match is found, the PDA determines the security privileges associated with the fingerprint (step 608) and determines if the e-mail function is among these privileges (step 609). If not, the method terminates (step 611); if it is, the PDA allows access to the e-mail function (step 610), and then terminates the authentication method (step 611).

[38] While the description above refers to particular embodiments of the present invention, it will be understood that many modifications may be made without departing from the spirit

thereof.

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A non-transitory computer-readable storage medium storing one or more programs comprising instructions, which when executed by an electronic device with a touch screen display, cause the device to:

display a plurality of icons on the touch screen display;

detect, with the touch screen display, a finger touch event, by a user, at a touch location on the touch screen display that corresponds to a location of a respective icon from the plurality of icons displayed on the touch screen display, wherein the respective icon is associated with a respective function; and

in response to detecting the finger touch event at the touch location on the touch screen display:

in accordance with a determination that the respective function does not require fingerprint authentication, authorize the respective function; and

in accordance with a determination that the respective function requires fingerprint authentication:

determine a plurality of security privileges of the user based on a comparison between a fingerprint detected during the finger touch event and previously stored fingerprint information; and

after determining the plurality of security privileges of the user, authorize the respective function when the plurality of security privileges of the user include a respective security privilege that indicates that the respective function is accessible to the user, wherein the plurality of security privileges of the user comprise a security privilege that indicates whether the user can access an electronic message that is received by the device from an external device.

2. The non-transitory computer-readable medium of claim 1, wherein the touch screen display is configured to capture the fingerprint of the user during the finger touch event.

3. The non-transitory computer-readable storage medium of claim 1, wherein:
the icon is an e-mail icon; and
the respective function is an e-mail function.
4. The non-transitory computer-readable storage medium of claim 3, wherein:
the computer-readable storage medium includes instructions for, prior to
detecting the finger touch event, receiving an e-mail which is secured for one or more
intended recipients; and
the plurality of security privileges of the user only include a security privilege that
indicates that the user can access the e-mail if the user is an intended recipient of the e-
mail.
5. The non-transitory computer-readable storage medium of claim 1, wherein the
previously stored fingerprint information includes stored images of fingerprints.
6. The non-transitory computer-readable storage medium of claim 1, wherein the
touch screen display includes a display selected from the set consisting of:
a liquid crystal display; and
a cathode ray tube display.
7. The non-transitory computer-readable storage medium of claim 1, wherein the
touch screen display includes a touch-sensitive surface selected from the set consisting
of:
a capacitive touch-sensitive surface;
an optical touch-sensitive surface;
an acoustic wave touch-sensitive surface in which acoustic waves are propagated
through the touch-sensitive surface; and
an acoustic wave touch-sensitive surface in which acoustic waves are propagated
on top of the touch-sensitive surface.
8. An electronic device, comprising:
a touch screen display;
one or more processors;
memory; and

one or more programs, wherein the one or more programs are stored in the memory and configured to be executed by the one or more processors, the one or more programs including instructions for:

displaying a plurality of icons on the touch screen display;

detecting, with the touch screen display, a finger touch event, by a user, at a touch location on the touch screen display that corresponds to a location of a respective icon from the plurality of icons displayed on the touch screen display, wherein the respective icon is associated with a respective function; and

in response to detecting the finger touch event at the touch location on the touch screen display:

in accordance with a determination that the respective function does not require fingerprint authentication, authorizing the respective function; and

in accordance with a determination that the respective function requires fingerprint authentication:

determine a plurality of security privileges of the user based on a comparison between a fingerprint detected during the finger touch event and previously stored fingerprint information; and

after determining the plurality of security privileges of the user, authorizing the respective function when the plurality of security privileges of the user include a respective security privilege that indicates that the respective function is accessible to the user, wherein the plurality of security privileges of the user comprise a security privilege that indicates whether the user can access an electronic message that is received by the device from an external device.

9. The device of claim 8, wherein the touch screen display is configured to capture the fingerprint of the user during the finger touch event.

10. The device of claim 8, wherein:
the icon is an e-mail icon; and
the respective function is an e-mail function.

11. The device of claim 10, wherein:
the device includes instructions for, prior to detecting the finger touch event, receiving an e-mail which is secured for one or more intended recipients; and

the plurality of security privileges of the user only include a security privilege that indicates that the user can access the e-mail if the user is an intended recipient of the e-mail.

12. The device of claim 8, wherein the previously stored fingerprint information includes stored images of fingerprints.

13. The device of claim 8, wherein the touch screen display includes a display selected from the set consisting of:

- a liquid crystal display; and
- a cathode ray tube display.

14. The device of claim 8, wherein the touch screen display includes a touch-sensitive surface selected from the set consisting of:

- a capacitive touch-sensitive surface;
- an optical touch-sensitive surface;
- an acoustic wave touch-sensitive surface in which acoustic waves are propagated through the touch-sensitive surface; and
- an acoustic wave touch-sensitive surface in which acoustic waves are propagated on top of the touch-sensitive surface.

15. A method, comprising:

- at an electronic device with a touch screen display:
 - displaying a plurality of icons on the touch screen display;
 - detecting, with the touch screen display, a finger touch event, by a user, at a touch location on the touch screen display that corresponds to a location of a respective icon from the plurality of icons displayed on the touch screen display, wherein the respective icon is associated with a respective function; and
 - in response to detecting the finger touch event at the touch location on the touch screen display:
 - in accordance with a determination that the respective function does not require fingerprint authentication, authorizing the respective function; and
 - in accordance with a determination that the respective function requires fingerprint authentication:

determine a plurality of security privileges of the user based on a comparison between a fingerprint detected during the finger touch event and previously stored fingerprint information; and

after determining the plurality of security privileges of the user, authorizing the respective function when the plurality of security privileges of the user include a respective security privilege that indicates that the respective function is accessible to the user, wherein the plurality of security privileges of the user comprise a security privilege that indicates whether the user can access an electronic message that is received by the device from an external device.

16. The method of claim 15, wherein the touch screen display is configured to capture the fingerprint of the user during the finger touch event.

17. The method of claim 15, wherein:
the icon is an e-mail icon; and
the respective function is an e-mail function.

18. The method of claim 17, wherein:
the method includes, prior to detecting the finger touch event, receiving an e-mail which is secured for one or more intended recipients; and
the plurality of security privileges of the user only include a security privilege that indicates that the user can access the e-mail if the user is an intended recipient of the e-mail.

19. The method of claim 15, wherein the previously stored fingerprint information includes stored images of fingerprints.

20. The method of claim 15, wherein the touch screen display includes a display selected from the set consisting of:
a liquid crystal display; and
a cathode ray tube display.

21. The method of claim 15, wherein the touch screen display includes a touch-sensitive surface selected from the set consisting of:
a capacitive touch-sensitive surface;

an optical touch-sensitive surface;

an acoustic wave touch-sensitive surface in which acoustic waves are propagated through the touch-sensitive surface; and

an acoustic wave touch-sensitive surface in which acoustic waves are propagated on top of the touch-sensitive surface.

DRAWINGS

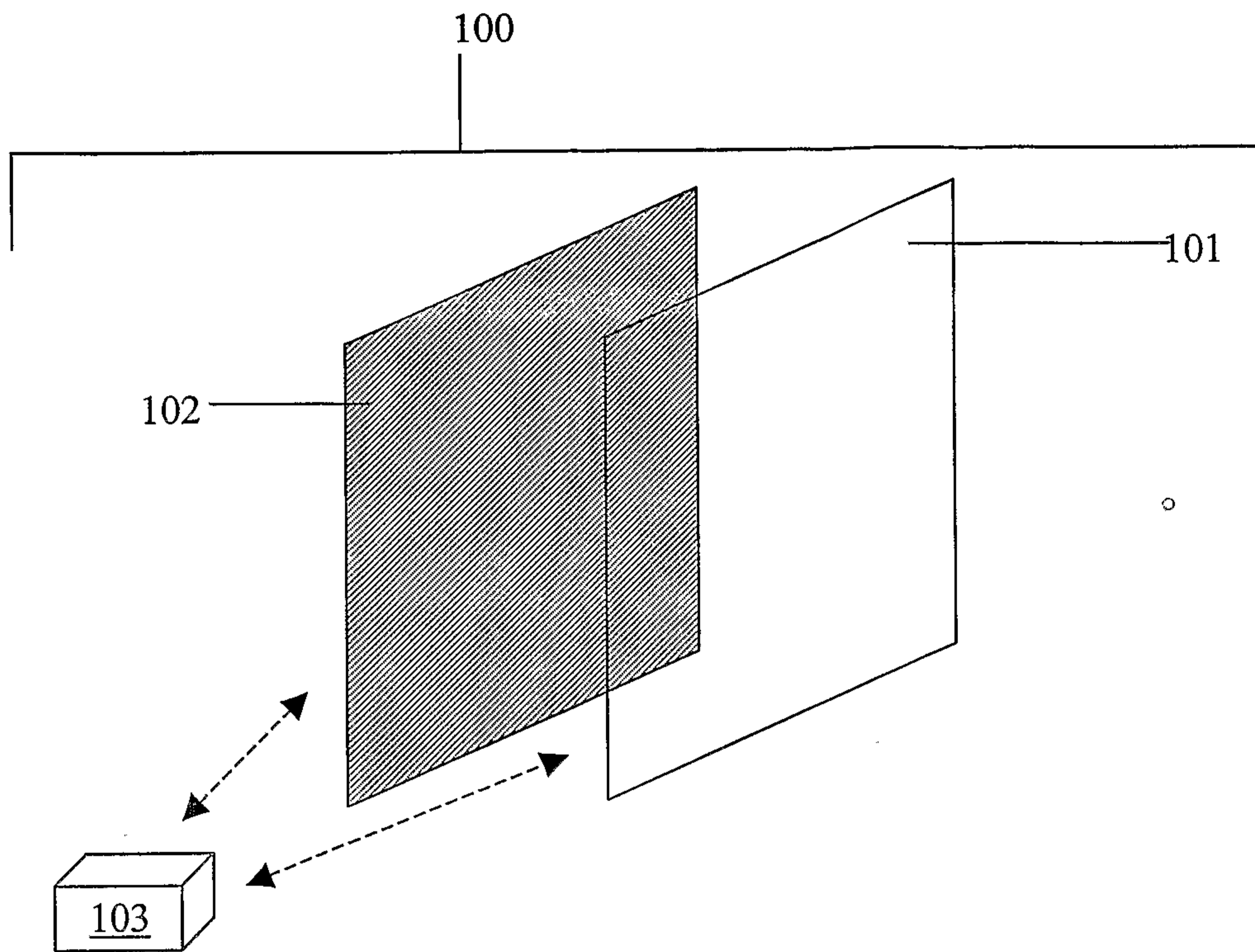


FIGURE 1

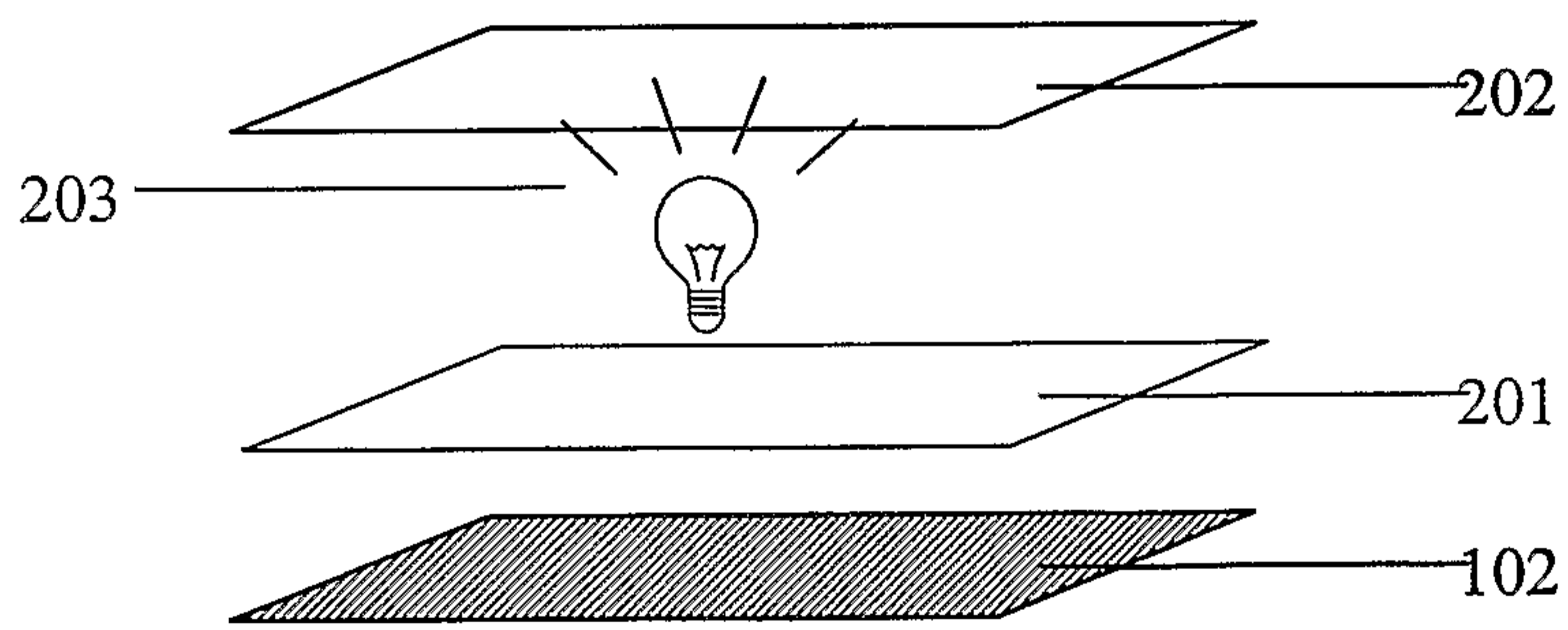


FIGURE 2

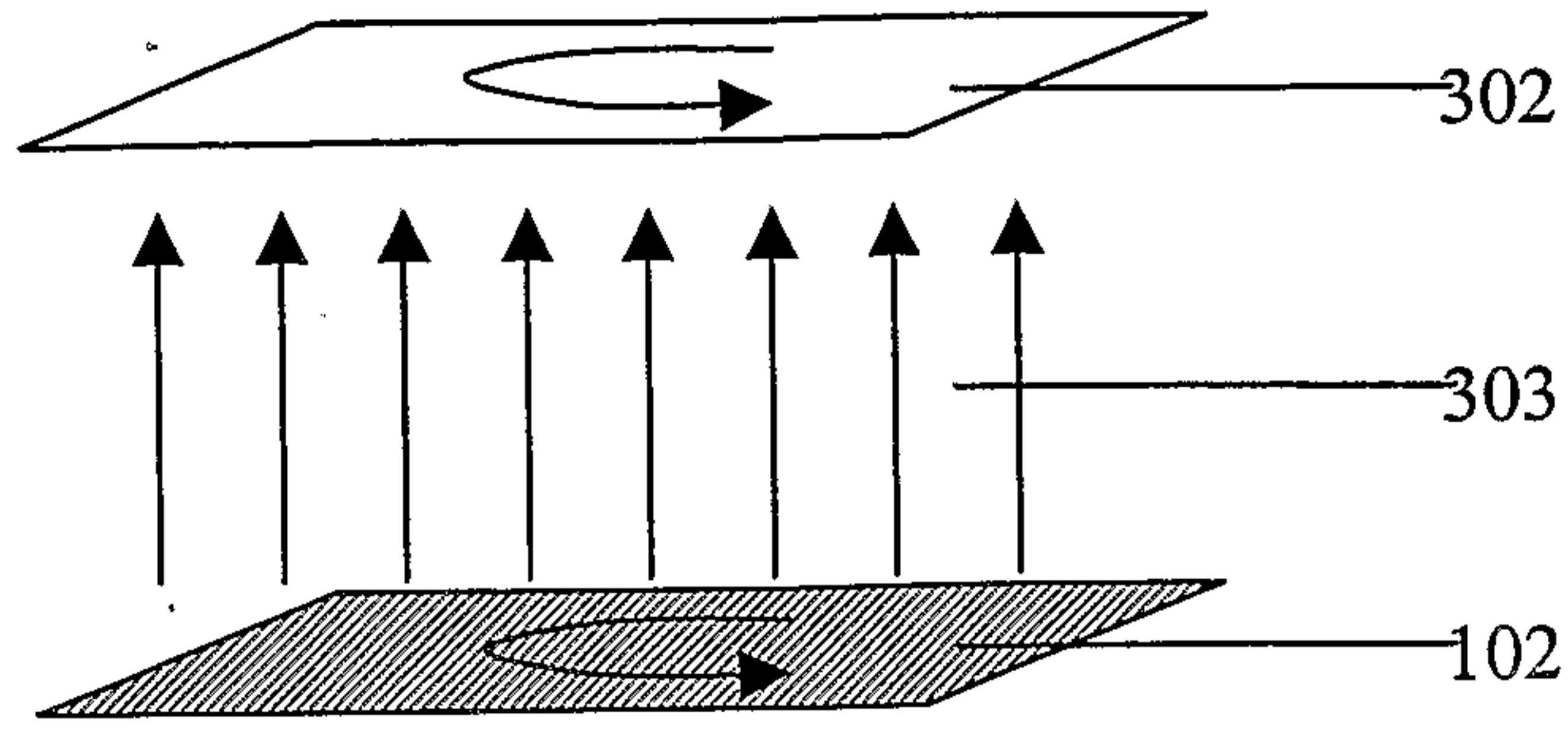


FIGURE 3

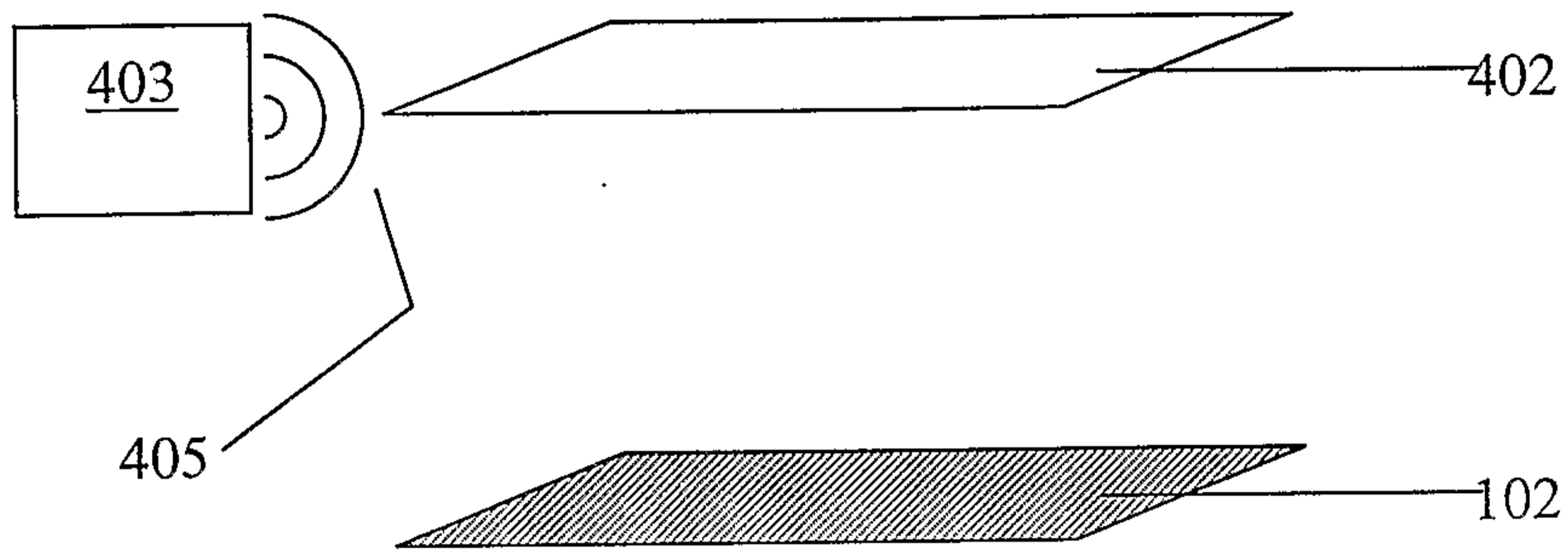


FIGURE 4

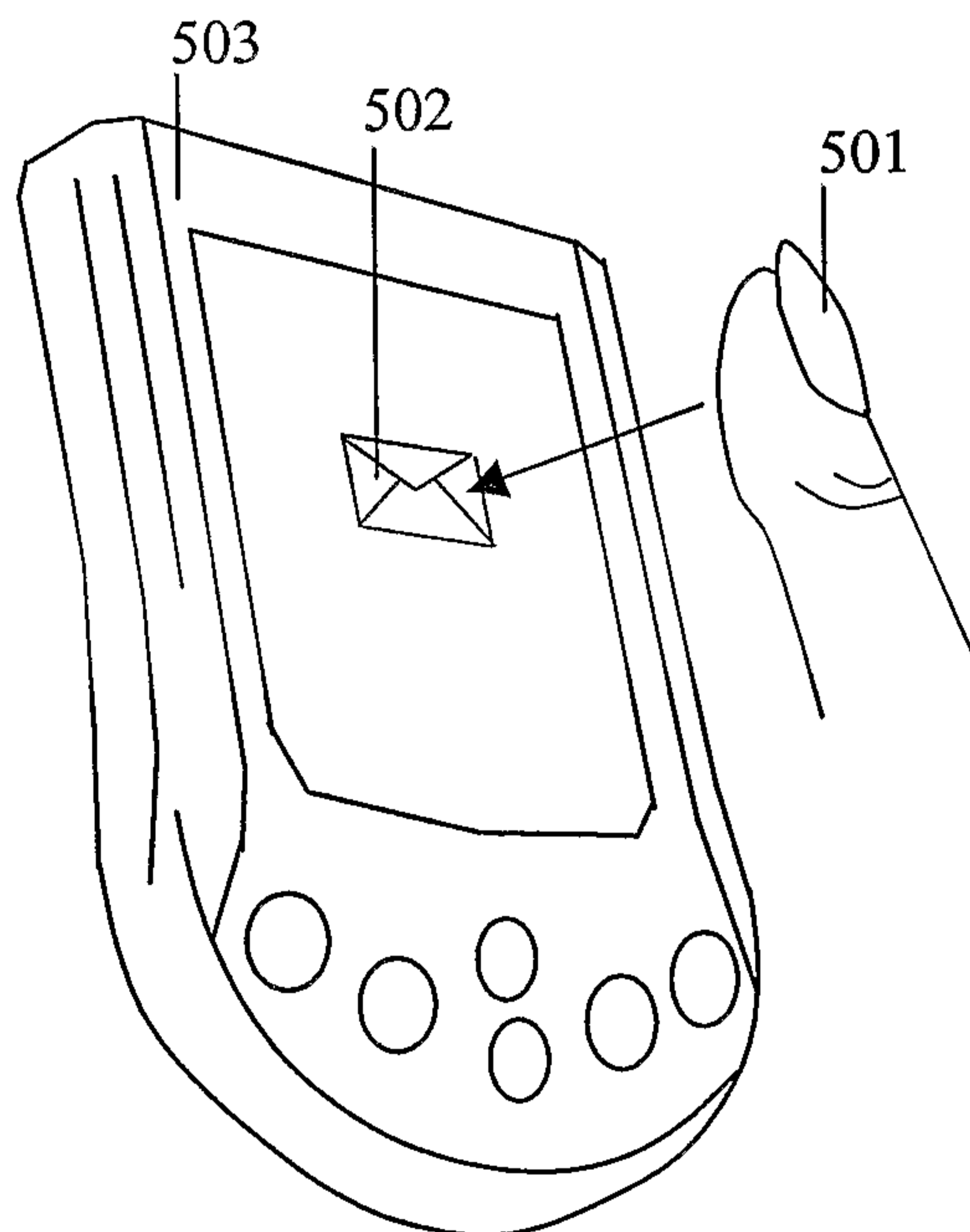


FIGURE 5

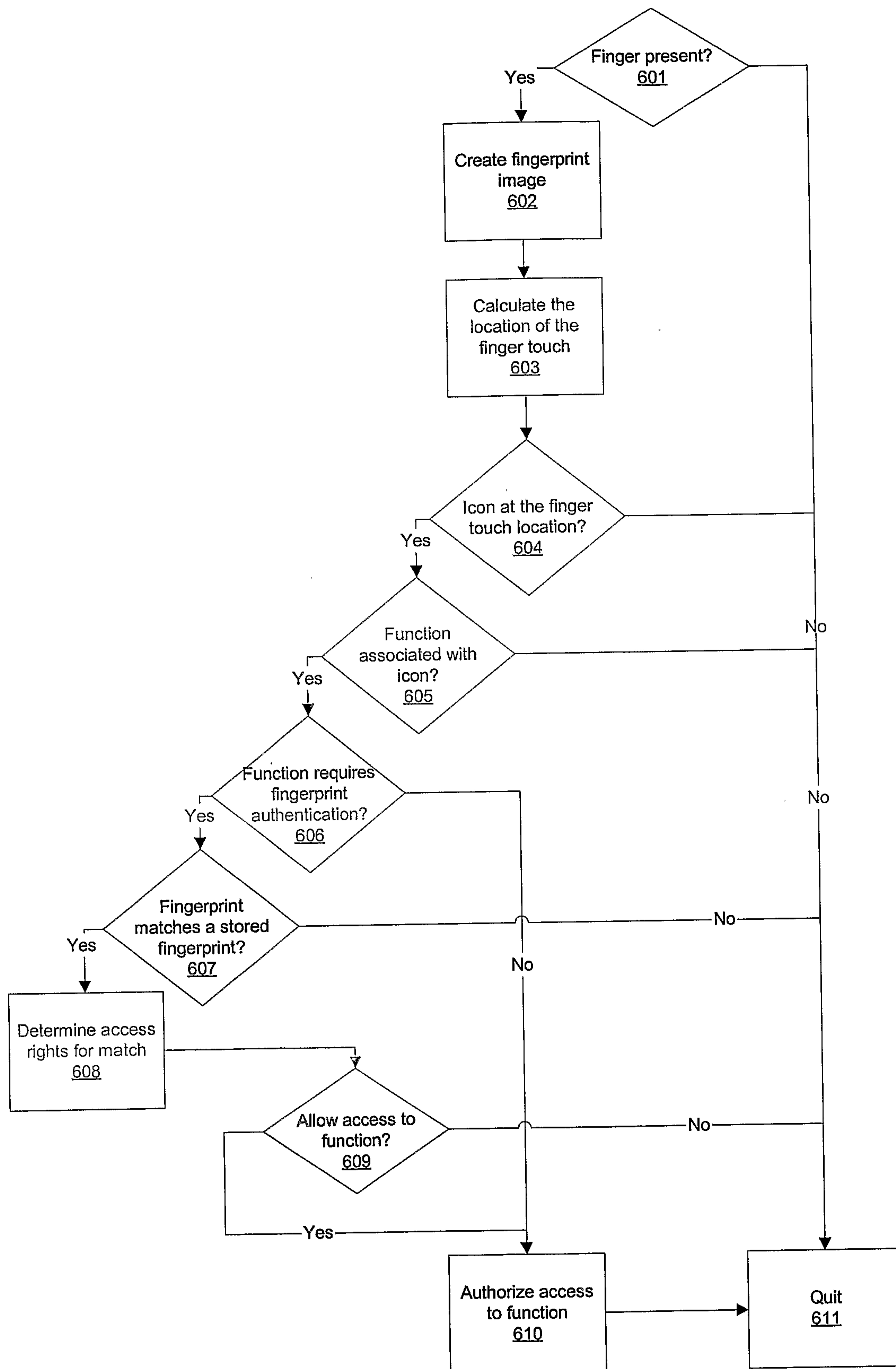


FIGURE 6

